# 目 录

# 第 1 章

# 关于 Baire 定理等的真假

在泛函分析教科书中，一般都有一条基础性的 Baire 定理，它是说："每个完备度量空间都是第二纲的". (例如可参看 [1], p37). 但在 1994 年的《Mathematical Reviews》中介绍说：N. Tsukada 在 1993 年构作了一些完备度量空间，它们不是第二纲的. (见该刊第 94f:54063 号评介). 以上似乎是两个互相矛盾的结果，但其实不然. 原因在于，这两个结果是分别在不同的集合论公理基础上得出的.

根据数理逻辑中关于公理集合论的研究，我们知道：在 E. Zermelo 与 A. A. Fraenkel 的集合论公理体系 ZF 基础上 (ZF 可以直观地看作人们通常所理解的朴素集合论，但不包含选择公理)，可以加用选择公理 AC, 也可以加用与之相反的"非 AC". (确切地说就是：如果 ZF 不矛盾，则"ZF+AC"和"ZF+(非 AC)"也都不矛盾.) 与此类似地，可以在 ZF 基础上加用一种比 AC 较弱的"相依选择公理"DC, 也可以加用与之相反的"非 DC". (确切地说就是：如果 ZF 不矛盾，则"ZF+DC"和"ZF+ 非 DC"也都不矛盾.) 关于这些，我们不在此证明，读者只须暂时承认即可. (其证明可参看 Th. Jech 的专著 [2]).

为了解释上述关于 Baire 定理的表面矛盾，我们在本章 §1 至 §5 中证明：在 ZF 基础上， Baire 第二纲定理是与 DC 等价的. 这原是 R. Goldblatt 在 1985 年的 [3] 中得到的结论，以下的论证主要就是由 [3] 中抽取素材而改写的.

另外，我们并在 §6 中附述一些性质类似的结果，涉及 Hahn-Banach 扩张定理以及 Lebesgue 测度方面一些情况.

根据各种不同的无矛盾性结果，如果有必要的话，我们完全可以在各该基础上发展内容不同的分析数学. 这正像欧氏几何与各种非欧几何间的关系一样. 所以，我们不能笼统地谈论一条命题的真假，只能谈论它在各种不同的无矛盾理论体系中的对错.

## §1 几个等价的命题

我们先写出几个命题，然后利用通常的朴素集合论 (即相当于 ZF) 证明它们的等价性.

**命题 1** (Baire 定理) 每个完备度量空间都是第二纲的.

**命题 2** 若 $(X,\rho)$ 是一个完备度量空间， $G_n(n=0,1,2,3,\cdots)$ 是 $X$ 中一系列稠密的开集，则 $\bigcap\limits_{n=0}^{\infty} G_n$ 在 $X$ 中稠密.

**命题 3** 若 $(P,\leqslant)$ 是一个偏序集， $D_n(n=0,1,2,3,\cdots)$ 是 $P$ 中一系列稠密的子集. (此时， $D\subseteq P$ 为稠密的含义是：对每个 $p\in P$ 都存在 $d\in D$ 能使 $d\leqslant p$). 则对每个 $p\in P$, 都存在一个序列 $f:\omega\longrightarrow P$ ($\omega$ 为自然数集) 能适合

$$\begin{cases}\text{(i) } f(0)=p;\\ \text{(ii) 对每一 } n\in\omega \text{ 都有 } f(n+1)\leqslant f(n);\\ \text{(iii) 对每一 } D_n, (f \text{ 的值域})\cap D_n \text{ 不空.}\end{cases}$$

**命题 4** (DC) 若 $A$ 是一个非空集合， $R$ 是 $A$ 上一个具有下

列性质的二元关系：

$$\text{对每一 } x \in A \text{ 都存在 } y \in A \text{ 适合 } xRy.$$

则对每个 $a \in A$ 都存在一个序列 $f: \omega \longrightarrow A$ 能适合：

$$\begin{cases} \text{(i) } f(0) = a; \\ \text{(ii) 对每一 } n \in \omega \text{ 都有 } f(n)Rf(n+1). \end{cases}$$

## §2 由命题 1 证命题 2

这是泛函分析书中常见的. 我们依据 [1] 简述如下：

$$\text{令 } A = X - \bigcap_{n=0}^{\infty} G_n = \bigcup_{n=0}^{\infty} (X - G_n). \tag{1}$$

对每个 $n \in \omega$, 由 $G_n$ 是 $X$ 中的稠密开集及 [1]p25 命题 1.4–4 知 $(X - G_n)$ 是在 $X$ 中疏朗的闭集. 从而由 (1) 及第一纲集定义 (见 [1]p26) 知 $A$ 是第一纲集. 再由 [1] 中 Baire 定理的推论 (见 [1]p38 第 2~3 行) 即知 $\bigcap_{n=0}^{\infty} G_n$ 在 $X$ 中稠密.

## §3 由命题 2 证命题 3

设 $(P, \leqslant)$ 是一个任意给定的 (非空) 偏序集.

(3.1) 以 $C$ 记一切适合下列性质的序列 $f: \omega \longrightarrow P$ 所成的集合：

$$f(0) \geqslant f(1) \geqslant f(2) \geqslant \cdots$$

在 $C$ 中定义一个度量 $d$ 如下：

$$\begin{cases} d(f,g) = \dfrac{1}{1 + (\text{使 } f(n) \neq g(n) \text{ 的最小 } n)}, & (\text{当 } f \neq g \text{ 时}); \\ d(f,g) = 0, & (\text{当 } f = g \text{ 时}). \end{cases}$$

易知 $(C,d)$ 构成一个度量空间. (例如当 $f,g,h$ 互异时, 可如下证明三角不等式: 令

$$k=(\text{使 } f(n)\neq g(n) \text{ 的最小 } n),$$
$$l=(\text{使 } g(n)\neq h(n) \text{ 的最小 } n),$$
$$m=(\text{使 } f(n)\neq h(n) \text{ 的最小 } n),$$
$$p=\min(k,l),$$

则易见 $p\leqslant m$. 从而有

$$d(f,g)+d(g,h)=\frac{1}{k+1}+\frac{1}{l+1}=\frac{1}{p+1}+\text{正数}$$
$$>\frac{1}{p+1}\geqslant\frac{1}{m+1}=d(f,h).$$

其他情况的验证更为显然.

下面证明度量空间 $(C,d)$ 是完备的.

设 $\{f_0,f_1,f_2,f_3,\cdots\}$ 为 $(C,d)$ 中任一 Cauchy 序列.

对每一自然数 $r$, 存在自然数 $N_r$ 能使当 $u,v\geqslant N_r$ 后有

$$d(f_u,f_v)<\frac{1}{r+1},$$

以 $N_r^*$ 记此种 $N_r$ 中之最小者. 又由 $d$ 的定义可知

$$(\text{使 } f_u(n)\neq f_v(n) \text{ 的最小} n)>r.$$

所以 $f_u,f_v$ 在 $\{0,1,\cdots,r\}$ 上的值相同. 特知:

$$f_{N_r^*},f_{N_r^*+1},f_{N_r^*+2},\cdots \text{在 } \{0,1,\cdots,r\} \text{ 上的值都相同}.$$

由以上又易见有 $N_0^*\leqslant N_1^*\leqslant N_2^*\leqslant\cdots$.

现在定义一个序列 $g:\omega\longrightarrow P$ 如下:

$$g(i)=f_{N_i^*}(i),\quad (i=0,1,2,3,\cdots)$$

则由诸 $f_i \in C$ 可知 $g \in C$, 这是因为

$$g(i) = f_{N_i^*}(i) = f_{N_{i+1}^*}(i) \geqslant f_{N_{i+1}^*}(i+1) = g(i+1).$$

(其中第二个 "=" 是根据上述, "$\geqslant$" 是由于 $f_{N_{i+1}^*} \in C$).

以下证明: $\{f_0, f_1, f_2, f_3, \cdots\}$ 按度量 $d$ 收敛于 $g$.

任给 $\varepsilon > 0$, 存在自然数 $r$ 使 $\frac{1}{r+1} < \frac{\varepsilon}{2}$. 当 $m \geqslant N_r^*$ 后, 有

$$d(f_m, f_{N_r^*}) < \frac{1}{r+1} \quad (\text{由 } N_r^* \text{ 取法}).$$

又由 $g$ 的定义易见 $g$ 与 $f_{N_r^*}$ 在 $\{0, 1, \cdots, r\}$ 上的值相同, 所以由 $d$ 的定义可知

$$d(g, f_{N_r^*}) < \frac{1}{r+1}.$$

由以上及 $d$ 的度量性质即知: 当 $m \geqslant N_r^*$ 后, 恒有

$$d(f_m, g) < \varepsilon.$$

(3.2) 设 $D_n$ $(n = 0, 1, 2, \cdots)$ 是 $P$ 中的一系列稠密子集.

对每个自然数 $n$, 令

$$S_n = \{f \in C \mid (f\text{的值集}) \cap D_n\text{不空}\}.$$

(3.2.1) 现在证明: $S_n$ 是 $(C, d)$ 中的开集.

任取 $f \in S_n$, 由 $S_n$ 定义可知存在一个最小的自然数 $m$ 能使 $f(m) \in D_n$. 以 $B(f, \dfrac{1}{m+1})$ 记 $C$ 中以 $f$ 为中心以 $\dfrac{1}{m+1}$ 为半径的开球. 以下说明 $B(f, \dfrac{1}{m+1}) \subseteq S_n$.

任取 $g \in B(f, \dfrac{1}{m+1})$, 则 $d(f, g) < \frac{1}{m+1}$, 从而易知 $g(m) = f(m) \in D_n$, 所以 $g \in S_n$.

(3.2.2) 再证 $S_n$ 是 $(C, d)$ 中的稠密子集.

任给 $f \in C$ 及 $C$ 中以 $f$ 为中心的任一开球 $B(f,\varepsilon)$ $(\varepsilon > 0)$.

取适合 $\frac{1}{m+1} < \varepsilon$ 的最小自然数 $m$. 由 $f \in C$ 有

$$f(0) \geqslant f(1) \geqslant \cdots \geqslant f(m).$$

再由 $D_n$ 在偏序集 $(P, \geqslant)$ 中的稠密性知存在 $p \in D_n$ 能使 $f(m) \geqslant p$.

现在定义 $h: \omega \longrightarrow P$ 如下:

$$\begin{cases} h(i) = f(i), & (\text{当 } i = 0, 1, \cdots, m); \\ h(i) = p, & (\text{当 } i = m+1, m+2, \cdots). \end{cases}$$

则 $h \in C$ 且 $p \in$ ($h$ 的值域)$\cap D_n$, 所以 $h \in S_n$. 又易见

$$d(f,h) < \frac{1}{m+1} < \varepsilon,$$

所以 $h \in B(f,\varepsilon)$. 从而 $S_n \cap B(f,\varepsilon)$ 不空.

(3.3) 由 (3.1) 及 (3.2) 及命题 2 可知

$$\bigcap_{n=0}^{\infty} S_n \text{ 在 } (c,d) \text{ 中稠密.} \tag{2}$$

对任意给定的 $p \in P$, 定义一个 $k: \omega \longrightarrow P$ 如下:

$$k(i) = p, \quad (i = 0, 1, 2, \cdots).$$

则 $k \in C$. 取 $C$ 中的开球 $B(k,1)$, 由 (2) 知

$$\left(\bigcap_{n=0}^{\infty} S_n\right) B(k,1) \text{ 不空.}$$

任取此交集中一元 $f$, 则:

(i) 由 $f \in B(k,1)$ 知 $d(f,k) < 1$, 从而 $f(0) = k(0) = p$;

(ii) 由 $f \in C$ 知: 对每一 $n \in \omega$ 都有 $f(n+1) \leqslant f(n)$;

(iii) 由 $f \in \bigcap_{n=0}^{\infty} S_n$ 知：对每个 $n \in \omega$, $f \in S_n$, 再由 $S_n$ 定义即知 ($f$ 的值域)$\cap D_n$ 不空.

## §4 由命题 3 证命题 4

设 $A$ 为一非空集合， $R$ 为 $A$ 上一个适合命题 4 题设的 2 元关系.

令 $P$ 为由一切如下的有限序列 $\langle a_0, a_1, \cdots, a_n\rangle$ 所构成的集合，其中诸 $a_i \in A$ 且适合：

$$a_0 R a_1, a_1 R a_2, \cdots, a_{n-1} R a_n.$$

$(n = 0, 1, 2, 3, \cdots)$.

对 $P$ 中的元素定义一个偏序 $\leqslant$ 如下：

$$(p \leqslant q)\text{当且只当}(q\text{ 是 }p\text{ 的一个前节}).$$

(也即：当且只当 $p = \langle a_0, a_1, \cdots, a_n\rangle$ 且 $q = \langle a_0, a_1, \cdots, a_m\rangle$ 且 $m \leqslant n$.)

再定义 $P$ 的诸子集 $D_n$ $(n = 0, 1, 2, \cdots)$ 如下：

$$D_n = \{p \in P \mid n \in (p\text{的定义域})\}.$$

对每个 $n$, 由关于 $R$ 的题设易见： $P$ 的任何元素 $q$ 都能扩张为 $D_n$ 中一个元素 $p$(即： $q$ 成为 $p$ 的一个前节), 从而 $q \geqslant p$. 所以， $D_n$ 是 $P$ 的稠密子集.

任意给定一个元素 $a \in A$ 之后，令 $p = \langle a\rangle \in P$. 由命题 3 知存在 $f: \omega \longrightarrow P$ 能适合

$$\begin{cases} f(0) = p = \langle a\rangle; \\ \text{对每一 } n \in \omega \text{ 都有： } f(n) \text{ 是 } f(n+1) \text{ 的前节}; \\ \text{对每一 } D_n, (f \text{ 的值域}) \cap D_n \text{ 不空}. \end{cases}$$

由以上性质及 $P$ 的定义即可看出，利用诸 $f(n)$ 可以在显然意义下合成一个序列 $g: \omega \longrightarrow A$ 使

$$\begin{cases} g(0)=a; \\ \text{对每一}\ \ m\in\omega\ \text{都有}\ \ g(m)Rg(m+1). \end{cases}$$

## §5 由命题 4 证命题 1 及总的结论

由命题 4 证命题 1, 可参看通常泛函分析教科书中的证法，例如 [1] p.37~p.38.

把 §2 至 §4 的内容与此结合起来，就知道：在 ZF 基础上，Baire 定理与 DC(以及与命题 2, 命题 3) 是等价的.

再与 §1 中所说的集合论结果结合起来，就知道：

一方面： (在 ZF 不矛盾的前题下)“ZF+(Baire 定理)” 不矛盾. 这就是通常数学书中的讲法.

另一方面： (在 ZF 不矛盾的前题下)“ZF+ 非 (Baire 定理)” 也不矛盾. 这就是 Tsukada 的构作的理论基础.

至于 ZF 的无矛盾性，可以说是至今公认的.

## §6 其他类似结果举例

在公理集合论与分析数学基础内容的关系方面，还有不少类似的研究，也都是值得注意的. 例如：

(I) 在泛函分析中有下列重要结论：

**命题 5** (Hahn–Banach 定理) 设 $p$ 为实线性空间 $E$ 上的实值亚线性泛函 (即适合 (i) 对一切 $x,y\in E, p(x+y)\leqslant p(x)+p(y)$ 及 (ii) 对一切 $x\in E$ 及正实数 $\alpha$, $p(\alpha x)=\alpha p(x)$). 若 $g$ 是定义在 $E$ 的一个子空间 $M$ 上的线性泛函，并且对一切 $x\in M$ 有 $g(x)\leqslant p(x)$, 则 $g$ 能扩展为 $E$ 上的线性泛函 $f$, 并且对一切 $x\in E$ 有 $f(x)\leqslant p(x)$.

对这一命题，也可以有与之相反的命题成立. 即：除了我们习知的“ZF+(Hahn-Banach 定理)”不矛盾之外，还可以造出另一种集合论模型来说明“ZF+ 非 (Hahn-Banach 定理)”也不矛盾 (可参看 [2] 及 [4]).

(II) 在 Lebesgue 测度与集合公理的关系方面，也有不少研究，这里只举一个值得注意的结果，就是：存在集合论模型 $M$，它不但适合 ZF 及 DC，并且在 $M$ 中实数集的每个子集都是 Lebesgue 可测的 (参看 [2] 及 [5]). 因而由 § 5 知在 $M$ 中也有 Baire 定理成立. 所以：“ZF+(Baire 定理)+ (实数集的每个子集都 Lebesgue 可测)”是不矛盾的. 如前所述，当必要时我们可以在这一基础上发展一种相应的分析数学. (但要注意这时不允许使用选择公理 AC，只能使用较弱的 DC. 因为由 AC 及 ZF 可以推出存在 Lebesgue 不可测的实数子集.) 对于其他各种已谈到或未谈到的无矛盾性结果，也都可以用这样的观点及态度来对待.

## 参考文献


1 孙永生. 泛函分析讲义. 北京：北京师范大学出版社，1986

2 Jech Th. The Axiom of Choice. Amsterdam: North-Holland Publ. Co., 1973

3 Goldblatt R. On the role of the Baire category theorem and dependent choice in the foundations of logic. Jour. Symbolic Logic, 1985, 50: 412~422

4 Pincus D. The strength of the Hahn-Banach theorem. Lecture Notes in Mathematics, 1974, 369: 203~248

5 Solovay R M. A model of set theory in which every set of reals is Lebesgue measurable. Annals of Math. (new series), 1970, 92: 1~56

# 第 2 章

# 具有物理意义的分球定理

在集合论中， S. Banach 和 A. Tarski 曾于 1924 年利用选择公理证明了一个在表面看来与人们的直觉不符的定理，其大意是说：3 维欧氏空间中的任一闭球体 $U$, 可以被分拆为有限个子集，然后把每个子集都看作刚体 (即：使每个子集内各点间的距离保持不变) 来重新拼装，能够得到两个与 $U$ 大小相同的闭球体！(从而也能继续改装成更多与 $U$ 同样大小的闭球体.) 这个定理，以前被称为 Banach–Tarski“分球怪论”，近来也有人称之为 Banach–Tarski“克隆”(见 [1]).

这个定理，也可被推广到 $n$ 维欧氏空间以及非球状的形体. 值得注意的是，它在近年来被赋予了各种物理意义. 例如：在专著 [2] 中，它被用于讨论量子力学方面的问题；在 [1] 中，将它用于讨论动力系统中的奇异吸引子问题.

作者无能力讨论这些物理解释及应用. 本章只是给出 3 维分球定理的证明，以供读者参考. 这一定理虽不是较新的结果，但由于以前它只被人们看成是选择公理的一种无用的“病态”推论，所以在一般书中都不提起或不加证明. 以下的证明是根据专著 [3] 改写的.

## §1 对球面的一种划分

设 $U$ 为 3 维欧氏空间中任一闭球，$d_1$ 与 $d_2$ 是 $U$ 的两个直径，其夹角为 $\theta$ $(0<\theta\leqslant\frac{\pi}{2})$. 以 $\varphi$ 记以 $d_1$ 为轴所作转角为 $\pi$ 的旋转，以 $\psi$ 记以 $d_2$ 为轴所作转角为 $\frac{2\pi}{3}$ 的旋转. ($d_1, d_2$ 的指向以及 $\varphi, \psi$ 的旋转方向都不影响以下的讨论，故可不作规定.) 我们要考虑由 $\varphi$ 和 $\psi$ 所生成的旋转群 $\Gamma_\theta$.

以 $G$ 记 2 元群 $\{1,a\}$ 及 3 元群 $\{1,b,b^2\}$ 的自由积. (也即：由生成元 $a,b$ 及定义关系 $a^2=1, b^3=1$ 所决定的群.)

**引理 1** 在上述记号下，存在 $d_1$ 与 $d_2$ 间的夹角 $\theta_1$，使由 $a\mapsto\varphi$，$b\mapsto\psi$ 所决定的由 $G$ 到 $\Gamma_{\theta_1}$ 上的同态映射是同构映射.

**证明** 考虑 $\Gamma_\theta$ 中任一元素 $\alpha$，显见它至少可以表示为下列诸形状之一：$\varphi^0, \varphi\cdot\psi^{\pm1}\cdot\cdots\cdot\varphi\cdot\psi^{\pm1}, \varphi\cdot\psi^{\pm1}\cdot\cdots\cdot\varphi, \psi^{\pm1}\cdot\varphi\cdot\cdots\cdot\psi^{\pm}\cdot\varphi$, $\psi^{\pm1}\cdot\varphi\cdot\cdots\cdot\psi^{\pm}$ (每个乘积只含有限个因子). 由此易见 $\Gamma_\theta$ 只含可数多个元素.

对于上述除 $\varphi^0$ 外 $\alpha$ 的每种可能形式，我们看相应的方程式 $\alpha=1$. 例如当 $\alpha=\varphi\cdot\psi^{-1}\cdot\varphi\cdot\psi$ 时，方程成为 $\varphi\cdot\psi^{-1}\cdot\varphi\cdot\psi=1$ 或 $\varphi\cdot\psi^2\cdot\varphi\cdot\psi=1$. (也即：围绕 $U$ 的中心连续作旋转 $\varphi,\psi,\psi,\varphi,\psi$ 后，要等于恒等变换，即使 $U$ 中每个点保持不变.) 由解析几何可知，这样的旋转轴夹角 $\theta$ $(0<\theta\leqslant\frac{\pi}{2})$ 只能有有限多种. 其他 $\alpha$ 仿此.

由以上两段，$\Gamma_\theta$ 中只含可数多个元素 $\alpha$，并且对每个 $\alpha$，只有 $d_1$ 与 $d_2$ 间的有限多种夹角 $\theta$ 能使相应的 $\alpha=1$ 成立. 但显见 $d_1$ 与 $d_2$ 间可以有不可数多种夹角 $\theta$. 所以存在 (很多)$d_1$ 与 $d_2$ 间的夹角 $\theta_1$ $(0<\theta_1\leqslant\frac{\pi}{2})$ 能使：在第一段中所述各种形状的乘积，除 $\varphi^0$ 外都不等于 1.

任取一组具有如上夹角 $\theta_1$ 的 $d_1$ 与 $d_2$，即易见由 $a \mapsto \varphi, b \mapsto \psi$ 所决定的由 $G$ 到 $\Gamma_{\theta_1}$ 上的同态映射是同构映射. (证毕)

以下，我们任意取定一组如上证末段所说的 $d_1$ 与 $d_2$，从而可以把与之相应的 $\Gamma_{\theta_1}$ 与 $G$ 等同起来. 因此，我们就把一组这样的旋转 $\{\varphi, \psi\}$ 看作 $G$ 的生成元组 $\{a, b\}$.

**引理 2** 在上述关于生成元的约定下，群 $G$ 可以划分为 3 个互不相交的子集 $A, B, C$，使： $G = A \cup B \cup C$ 并且

$$A \cdot \varphi = B \cup C, \quad A \cdot \psi = B, \quad A \cdot \psi^2 = C. \tag{1}$$

**证明** 我们对 $G$ 的元素按其长度归纳地定义 $A, B, C$ 如下.

首先，令 $1 \in A$; $\varphi, \psi \in B$; $\psi^2 \in C$. 然后，按下述规则确定 $G$ 中每一元素的归属：

若 $\alpha$ 的最右因子为 $\psi^{\pm 1}$. 令 $\alpha\varphi \in B$ (当 $\alpha \in A$), $\alpha\varphi \in A$ (当 $\alpha \in B$), $\alpha\varphi \in A$ (当 $\alpha \in C$).

若 $\alpha$ 的最右因于为 $\varphi$. 令 $\alpha\psi \in B$ (当 $\alpha \in A$), $\alpha\psi \in C$ (当 $\alpha \in B$), $\alpha\psi \in A$ (当 $\alpha \in C$), $\alpha\psi^{-1} \in C$ (当 $\alpha \in A$), $\alpha\psi^{-1} \in A$ (当 $\alpha \in B$), $\alpha\psi^{-1} \in B$ (当 $\alpha \in C$).

对于这样定义的 $A, B, C$，易见其互不相交，并且适合 $G = A \cup B \cup C$ 及 (1) 中三个等式. (证毕)

**定理 1** 设 $S$ 为 3 维欧氏空间中任一球面，则 $S$ 可以划分为 4 个互不相交的子集 $A_1, B_1, C_1, Q$ 使适合 $S = A_1 \cup B_1 \cup C_1 \cup Q$ 及

(i) $A_1, B_1, C_1$ 彼此合同.

(ii) $B_1 \cup C_1$ 合同于 $A_1, B_1, C_1$.

(iii) $Q$ 为可数集.

**证明** 以 $U$ 记与 $S$ 相应的闭球，并考虑前述的群 $G$(视为与 $U$ 相应的一个旋转群 $\Gamma_{\theta_1}$). 对于每个 $\alpha \in G$，与之相应的旋转在 $S$ 上恰有两个不动点. 当 $\alpha$ 跑遍 $G$ 时，这些不动点组成 $S$ 的一个可数子集 $Q$(注意 $G$ 为可数).

在点集 $S$-$Q$ 中引入一关系 $\sim$ 如下："$x \sim y$" 当且只当 "存在 $\alpha \in G$ 使 $x\alpha = y$".

易见 $\sim$ 是一等价关系，它把 $S$-$Q$ 划分为一族等价类. 利用选择公理，可以由每一等价类中取出一个元素作代表，以 $M$ 记这些代表所组成的集.

现在令

$$A_1 = M \cdot A, \quad B_1 = M \cdot B, \quad C_1 = M \cdot C.$$

其中 $A, B, C$ 如引理 2 所述. 则由引理 2 易知：$S = A_1 \cup B_1 \cup C_1 \cup Q$; $A_1, B_1, C_1, Q$ 互不相交；$A_1, B_1, C_1$ 彼此合同；并且 $B_1 \cup C_1$ 与 $A_1, B_1, C_1$ 合同. (证毕)

## §2 闭球体的克隆定理

**定义** 以 $\mathbf{R}^3$ 记 3 维欧氏空间. 在 $\mathbf{R}^3$ 的诸子集间定义关系 $\approx$ 如下：对任何 $X, Y \subseteq \mathbf{R}^3$，令 "$X \approx Y$" 当且只当 "存在一正整数 $m$，使 $X, Y$ 各能划分为 $m$ 个互不相交子集的并：$X = X_1 \cup \cdots \cup X_m$，$Y = Y_1 \cup \cdots \cup Y_m$；并且每个 $X_i$ 与相应的 $Y_i$ 合同 $(i = 1, \cdots, m)$".

**引理 3** $\mathbf{R}^3$ 上的关系 $\approx$ 具有下列性质：

(i) $\approx$ 是等价关系.

(ii) 设 $X = X_1 \cup X_2$, $X_1 \cap X_2 = \phi$(空集), $Y = Y_1 \cup Y_2$, $Y_1 \cap Y_2 = \phi$. 若 $X_i \approx Y_i$ $(i = 1, 2)$，则 $X \approx Y$.

(iii) 若 $X_1 \subseteq Y \subseteq X$ 且 $X \approx X_1$，则 $X \approx Y$.

**证明** (i),(ii) 易见. 以下证 (iii).

由 $X \approx X_1$ 知存在正整数 $n$ 及 $X, X_1$ 的划分能使 $X = X^1 \cup \cdots \cup X^n$(诸 $X^i$ 互不相交) 及 $X_1 = X_1^1 \cup \cdots \cup X_1^n$ (诸 $X_1^i$ 互不相交) 并且 $X^i$ 与 $X_1^i$ 合同 $(i = 1, \cdots, n)$.

对每个 $i(1 \leqslant i \leqslant n)$ 取定一个合同映射 $f^i: X^i \longrightarrow X_1^i$, 则由这些合同映射可以合成一个由 $X$ 到 $X_1$ 上的 1–1 映射 $f$.

现在令

$$X_0 = X,\ X_1 = f(X_0),\ X_2 = f(X_1), \cdots;$$
$$Y_0 = Y,\ Y_1 = f(Y_0),\ Y_2 = f(Y_1), \cdots$$

其中 $f(X_0) = \{f(x): x \in X_0\}$, 其他仿此 (注意由 $X_1 \subseteq Y \subseteq X$ 易见诸 $X_j, Y_j$ 有意义). 并令

$$Z = \bigcup_{j=0}^{\infty} (X_j - Y_j).$$

则有下列诸事实:

(I) $f(Z)$ 与 $X - Z$ 不相交. 因: 若 $y \in f(Z)$, 则存在 $z \in Z$ 使 $y = f(z)$. 设 $z \in X_k - Y_k$, 则 $f(z) \in f(X_k) = X_{k+1}$, 又由 $z \notin Y_k$ 及 $f$ 为 1–1 可知 $f(z) \notin f(Y_k) = Y_{k+1}$, 所以 $f(z) \in Z$, 从而 $y \notin X - Z$.

(II) $Z \approx f(Z)$. 理由如下: 令

$$Z^i = Z \cap X^i,\quad Z_1^i = f(Z) \cap X_1^i,\quad (i = 1, \cdots, n).$$

由 $Z \subseteq X$ 易见有 $Z = Z^1 \cup \cdots \cup Z^n$(诸 $Z^i$ 互不相交) 以及 $f(Z) \subseteq f(X) = X_1$, 从而又有 $f(Z) = Z_1^1 \cup \cdots \cup Z_1^n$ (诸 $Z_1^i$ 互不相交). 又由 $f$ 的定义可知 $f^i(Z^i) = f(Z^i) = f(Z) \cap f(X^i) = f(Z) \cap f^i(X^i) = f(Z) \cap X_1^i = Z_1^i$, 故由 $f^i$ 为合同映射知 $Z^i$ 与 $Z_1^i$ 合同 $(i = 1, \cdots, n)$.

(III) $X = Z \cup (X - Z)$ 且 $Y = f(Z) \cup (X - Z)$. 前者显然, 后者证明如下: (3.1) 由 $Z \subseteq X$ 有 $f(Z) \subseteq f(X) = X_1 \subseteq Y$. 又若 $x \in X - Z$, 则 $x \notin Z$, 所以 $x \notin X_0 - Y_0 = X - Y$, 从而 $x \in Y$. 由以上有 $f(Z) \cup (X - Z) \subseteq Y$. (3.2) 任取 $y \in Y$. 若 $y \notin X - Z$, 则 $y \in Z$, 所以存在自然数 $k$ 使 $y \in X_k - Y_k$, 且由 $y \in Y = Y_0$ 知 $k > 0$. 再

由 $X_k$ 及 $Y_k$ 定义及 $f$ 为 1–1 可知存在 $z \in X_{k-1} - Y_{k-1} \subseteq Z$ 使 $y = f(z) \in f(Z)$. 由以上有 $Y \subseteq f(Z) \cup (X - Z)$.

由 (I),(II),(III) 及 (ii) 即知 $X \approx Y$. (证毕)

**定理 2**(Banach–Tarski 定理) 设 $U$ 为 3 维欧氏空间中任一闭球，则 $U$ 可被划分为两个互不相交子集 $X, Y$ 的并 $U = X \cup Y$ 使得 $X \approx U$ 且 $Y \approx U$.

**证明** (I) 以 $S$ 记 $U$ 的表面球，并设

$$S = A_1 \cup B_1 \cup C_1 \cup Q$$

为依定理 1 对 $S$ 所作的划分. 由此可得 $U$ 的一个划分如下:

$$U = \overline{A}_1 \cup \overline{B}_1 \cup \overline{C}_1 \cup \overline{Q} \cup \{c\}. \tag{1}$$

其中: $c$ 是 $U$ 的球心; $\overline{A}_1$ 是由 $A_1$ 中各点所决定的半径上诸点 (除 $c$ 外) 所构成的锥体; $\overline{B}_1, \overline{C}_1, \overline{Q}$ 仿此.

由 $A_1, B_1, C_1$ 的取法 (见定理 1) 可知有:

$$\overline{A}_1, \overline{B}_1, \overline{C}_1, \overline{B}_1 \cup \overline{C}_1 \text{ 彼此合同.} \tag{2}$$

现在令

$$X = \overline{A}_1 \cup \overline{Q} \cup \{c\}, \quad Y = U - X. \tag{3}$$

(II) 由 (2) 及引理 3 之 (i),(ii) 可得

$$\overline{A}_1 \approx \overline{B}_1 \cup \overline{C}_1 \approx \overline{A}_1 \cup \overline{C}_1 \approx \overline{A}_1 \cup \overline{B}_1 \cup \overline{C}_1. \tag{4}$$

再由 (1) 及 (3) 即见有 $X \approx U$.

(III) 由于点集 $Q$ 为可数，并且以 $c$ 为中心的旋转群 $G$ 也可数，故易见存在一个以 $c$ 为中心的旋转 $\alpha (\notin G)$ 能使 $Q$ 与 $Q \cdot \alpha$ 不相交. 从而由 $S = A_1 \cup B_1 \cup C_1 \cup Q$ 知

$$Q \cdot \alpha \subseteq A_1 \cup B_1 \cup C_1. \tag{5}$$

又仿 (4) 有

$$\overline{C}_1 \approx \overline{A}_1 \cup \overline{B}_1 \cup \overline{C}_1. \tag{6}$$

由 (5),(6) 易知存在 $C_1$ 的可数子集 $S_1$ 能使

$$\overline{S}_1 \approx \overline{Q \cdot \alpha}.$$

从而也有

$$\overline{S}_1 \approx \overline{Q}. \tag{7}$$

再任取 $\overline{C}_1 - \overline{S}_1$ 中一点 $p$.(因 $S_1$ 可数而由定理 1 易知 $C_1$ 不可数，故知 $p$ 存在.) 则易见有

$$X = \overline{A}_1 \cup \overline{Q} \cup \{c\} \approx \overline{B}_1 \cup \overline{S}_1 \cup \{p\}.$$

从而由 (II) 有

$$\overline{B}_1 \cup \overline{S}_1 \cup \{p\} \approx U. \tag{8}$$

但由 $Y$ 的定义及 $S_1$ 和 $p$ 的取法又有

$$\overline{B}_1 \cup \overline{S}_1 \cup \{p\} \subseteq Y \subseteq U.$$

再由 (8) 及引理 3 之 (iii) 即得 $Y \approx U$.　　(证毕)

## 参考文献


1 Svozil K. Set theory and physics. Foundations of Physics, 1995, 25: 1541~1560

2 Pitowsky I. Quantum Probability–Quantum Logic. Berlin: Springer–Verlag, 1989

3 Jech Th. The Axiom of Choice. Amsterdam: North–Holland Publ. Co., 1973

# 第 3 章

# 二次数环的 Hilbert 第 10 问题

Hilbert 第 10 问题是著名数学家 D. Hilbert 于 1900 年提出的 23 个问题之一．它是问：能否设计一个有效的方法，使得对每个整系数不定方程都能用此方法在有限多步内判定它是否有整数解？对于这一问题，经过人们的多年研究，到 1970 年，才由 Y. Matijasevitch 在 M. Davis, H. Putnam 及 J. Robinson 等人应用递归论方法对此问题所作研究的成果基础上，最后证明了它的递归不可解性，即：不存在递归性的方法，使得对每个整系数不定方程都能用此方法判定它是否有整数解．（按照一般观点，递归性就是对直观上所谓有效性的数学反映．这是首先由 A. Church 提出的，被称为 Church 论断.）关于这一著名的“递归不可解”结果的介绍，可参看文献 [1] 或 [2].

在这一结果的基础上，人们又对 Hilbert 第 10 问题作了不少推广，研究关于一些代数整数环，多项式环，有理函数域等的类似问题，得到不少类似的结果．关于这方面的推广研究，可参看文献 [3] 中的综述.

本章讨论关于二次代数整数环的 Hilbert 第 10 问题，也就是问：设 $R(\sqrt{D})$ 是一个给定的二次数环，能否设计一个有效的方

法，使得对每个整系数不定方程都能用此方法在有限多步内判定它在 $R(\sqrt{D})$ 中是否有解？以下将介绍 J. Denef 对此问题的解答，就是：对每个二次数环 $R(\sqrt{D})$，其 Hilbert 第 10 问题都是递归不可解的. 证明的方法主要是通过对二次数环性质的讨论，把问题化归到自然数系的 Hilbert 第 10 问题 (易知后者与 Hilbert 原来的第 10 问题等价). 本章并不直接用到递归论的知识. 以下的介绍，是根据 Denef 的原始文献 [4]，并对之作了较详细的补充说明.

以下以 $\mathbf{N}, \mathbf{Z}$ 及 $\mathbf{Q}$ 分别记自然数系 (包括 0 在内)，整数环及有理数域.

**引理 1** 设 $P$ 为一非平方自然数，则存在自然数 $X, Y (Y \neq 0)$ 能适合 Pell 方程 $X^2 - PY^2 = 1$.

证明见各数论书.

**定义** 对任一自然数 $A > 1$ 及任一自然数足码 $n$，以 $X_n(A)$，$Y_n(A)$ 记由下列等式所决定的自然数：

$$X_n(A) + Y_n(A)\sqrt{A^2 - 1} = (A + \sqrt{A^2 - 1})^n.$$

(当 $A$ 确定时，以下也把 $X_n(A), Y_n(A)$ 简记为 $X_n, Y_n$).

**引理 2** 对任何自然数 $A > 1$，设 $P = A^2 - 1$，则 Pell 方程 $X^2 - PY^2 = 1$ 的全部自然数解为

$$X = X_n(A), \quad Y = Y_n(A). \quad (n = 0, 1, 2, \cdots)$$

证明见各数论书.

**引理 3** 设自然数 $A > 1$，则对任何自然数 $n, k$ 都有

$$(Y_{nk}(A))^2 \equiv (Y_n(A))^2 k^2, \quad (\mathrm{mod}(Y_n(A))^4).$$

**证明** 当 $n = 0$ 或 $k = 0$ 时，易见结论为真. 以下设 $n > 0$ 且 $k > 0$.

习知

$$Y_{nk} = \sum_{j=1;j\,\text{奇}}^{k} \binom{k}{j} (A^2 - 1)^{\frac{j-1}{2}} X_n^{k-j} Y_n^j,$$

故有 $Y_{nk} \equiv kX_n^{k-1}Y_n \pmod{Y_n^3}$ 及 $(Y_{nk}/Y_n) \equiv kX_n^{k-1} \pmod{Y_n^2}$. 两端平方，得

$$(Y_{nk}/Y_n)^2 \equiv k^2(X_n^2)^{k-1} \pmod{Y_n^2}.$$

但由引理 2 有

$$X_n^2 \equiv 1 \pmod{Y_n^2},$$

从而即得所欲证. (证毕)

## §1 实二次数环的情况

在本节中，设整数 $D > 1$ 无平方因子. 以 $R(\sqrt{D})$ 记二次数域 $\mathbf{Q}(\sqrt{D})$ 中全体代数整数所成的二次数环.

**引理 4** 设自然数 $A, B$ $(B \neq 0)$ 适合 Pell 方程 $A^2 - DB^2 = 1$, 令 $E = A^2 - 1$. 若 $x, y \in R(\sqrt{D})$ 适合

$$x^2 - Ey^2 = 1,$$

则 $y^2 \in N$.

**证明** 显见有 $A > 1$ 及 $E = B^2D$, 从而有

$$(x + B\sqrt{D}y)(x - B\sqrt{D}y) = 1,$$

所以 $x + B\sqrt{D}y$ 是 $R(\sqrt{D})$ 中的单位.

令 $u = x + B\sqrt{D}y$, 则 $u^{-1} = x - B\sqrt{D}y$. 将此二式相减并两端平方，得

$$4B^2Dy^2 + 2 = u^2 + u^{-2}.$$

又由 $u$ 为单位知其范数 $N(u)=\pm1$, 从而有 $u^{-1}=\pm\overline{u}$ ($\overline{u}$ 为 $u$ 在 $R(\sqrt{D})$ 中的共轭元). 故得

$$4B^2Dy^2+2=u^2+(\overline{u})^2\in\mathbf{Q},$$

从而 $y^2\in\mathbf{Q}$.

但 $y^2\in R(\sqrt{D})$, 所以 $y^2\in\mathbf{Z}$. 又因 $D>1$, 所以 $y^2\in N$. (证毕)

**引理 5** 设 $x,y,z\in R(\sqrt{D})$. 若 $x\equiv y(\mathrm{mod}\,z)$ 并且 $0\leqslant x<z$, $0\leqslant\overline{x}<\overline{z}$, $0\leqslant y<z$, $0\leqslant\overline{y}<\overline{z}$, 则 $x=y$. (此处 $x\equiv y(\mathrm{mod}\,z)$ 表示: 存在 $w\in R(\sqrt{D})$ 使 $x-y=wz$.)

**证明** 由题设知存在 $w\in R(\sqrt{D})$ 使 $x-y=wz$, 从而有

$$|x-y|\cdot|\overline{x}-\overline{y}|=|w\overline{w}|\cdot|z\overline{z}|=|N(w)|\cdot|z\overline{z}|.$$

假若 $x\neq y$, 则 $w\neq0$, $|N(w)|\geqslant1$, 从而有

$$|x-y|\cdot|\overline{x}-\overline{y}|\geqslant|z\overline{z}|,$$

但易见这与题设中诸不等式矛盾. (证毕)

**引理 6** 依引理 4 的题设取一自然数 $E$. 令 $\Sigma$ 为下列不定方程组 (以 $t,x,y,u,v,z,w,h,q,r,s$ 为未知数):

$$\Sigma\begin{cases}\text{(a)}\ \ x^2-Ey^2-1=0,\\ \text{(b)}\ \ u^2-Ev^2-1=0,\\ \text{(c)}\ \ v^2-y^2t-zy^4=0,\\ \text{(d)}\ \ t-w^2=0,\\ \text{(e)}\ \ y^2-h^2-q^2-r^2-s^2-t-1=0.\end{cases}$$

则有下列二结论成立:

(i) 若 $\Sigma$ 在 $R(\sqrt{D})$ 中有解为 $\langle t,x,\cdots,s\rangle$, 则 $t\in\mathbf{Z}$.

(ii) 若 $k$ 为一自然数, 则 $\Sigma$ 在 $R(\sqrt{D})$ 中有一组解 $\langle t, x, \cdots, s\rangle$, 其中 $t = k^2$.

**证明** (I) 先证 (i). 已知 $t, x, \cdots, s \in R(\sqrt{D})$ 适合 $\Sigma$. 由 (d),(e) 及 $R(\sqrt{D})$ 为实可知 $y \neq 0$. 再由 (c) 有 $y^2 | v^2$ 及

$$(v^2/y^2) \equiv t \pmod{y^2}. \tag{1}$$

由 (a),(b) 及引理 4 有 $y^2 \in N$ 及 $v^2 \in \mathbf{N}$, 故由 (1) 又可得 $(v^2/y^2) \equiv \bar{t} \pmod{y^2}$, 从而有

$$t \equiv \bar{t} \pmod{y^2}. \tag{2}$$

又由 (d),(e) 及 $R(\sqrt{D})$ 为实可知

$$0 \leqslant t < y^2. \tag{3}$$

对 (d),(e) 取共轭式, 仿上又可得

$$0 \leqslant \bar{t} < (\bar{y})^2 = y^2. \tag{4}$$

由 (2),(3),(4) 及引理 5 可得 $t = \bar{t}$, 从而 $t \in \mathbf{Z}$.

(II) 再证 (ii). 已知 $k \in \mathbf{N}$, 现在对于依引理 4 的题设取 $E$ 时所用的 $A$, 任意取定一个足码 $n$ 使 $Y_n(A) > k$(由 $Y_n(A)$ 定义易知此种 $n$ 存在).

令 $t = k^2$, $x = X_n$, $y = Y_n$, $u = X_{nk}$, $v = Y_{nk}$, $w = k$. 则 (d) 已成立; 由引理 2 知 (a) 及 (b) 成立; 由引理 3 知存在 $z \in R(\sqrt{D})$ 使 (c) 成立.

最后, 由 $y > k \geqslant 0$ 可知 $y^2 - t = y^2 - k^2$ 为正整数, 故由 Lagrange 定理可知又存在 $h, q, r, s \in \mathbf{Z} \subseteq R(\sqrt{D})$ 使 (e) 成立. (证毕)

把 $\Sigma$ 中 (a) 至 (e) 左端的多项式各记为 $p_1(t, x, \cdots, s), \cdots, p_5(t, x, \cdots, s)$. 以 $P_1(n, k_1, \cdots, k_4, t_1, x_1, \cdots, s_1, \cdots, t_4, x_4, \cdots, s_4)$ 记

下列多项式：

$$(n-t_1-\cdots-t_4)^2+\sum_{j=1}^{4}\left[(p_1(t_j,x_j,\cdots,s_j))^2+\cdots\right.$$
$$\left.+(p_5(t_j,x_j,\cdots,s_j))^2+(t_j-k_j^2)^2\right].$$

**定理 1** 设 $n\in R(\sqrt{D})$, $(D>1)$, 则 $n\in N$ 的充分必要条件是：存在 $k_1,\cdots,k_4,t_1,x_1,\cdots,s_1,\cdots,t_4,x_4,\cdots,s_4\in R(\sqrt{D})$ 使 $P_1(n,k_1,\cdots,k_4,t_1,x_1,\cdots,s_1,\cdots,t_4,x_4,\cdots,s_4)=0$.

**证明** (I) 设存在 $k_1,\cdots,k_4,t_1,x_1,\cdots,s_1,\cdots,t_4,x_4,\cdots,s_4\in R(\sqrt{D})$ 使 $P_1=0$. 注意到 $R(\sqrt{D})$ 为实二次数环，则由 $P_1$ 的构成及引理 6(i) 知诸 $t_j\in\mathbf{Z}$. 又由 $P_1=0$ 知 $n=t_1+\cdots+t_4$ 并且诸 $t_j=k_j^2$, 所以诸 $t_j\in\mathbf{N}$, 从而 $n\in\mathbf{N}$.

(II) 反之，设 $n\in N$. 则由 Lagrange 定理知 $n$ 可以表示为 4 个自然数 $k_1,\cdots,k_4$ 的平方和. 令诸 $t_j=k_j^2$, 则有 $n=t_1+\cdots+t_4$. 对每个 $j$, 由引理 6(ii) 知在 $R(\sqrt{D})$ 中存在 $x_j,\cdots,s_j$ 使与 $t_j$ 一起适合 $\Sigma$. 由以上及 $P_1$ 的构成即见有

$$P_1(n,k_1,\cdots,k_4,t_1,x_1,\cdots,s_1,\cdots,t_4,x_4,\cdots,s_4)=0. \qquad \text{(证毕)}$$

**定理 2** 设 $R(\sqrt{D})$ 为任一实二次数环，则其 Hilbert 第 10 问题递归不可解.

**证明** 假设 $R(\sqrt{D})$ 的 Hilbert 第 10 问题递归可解，则存在一个相应的判定算法 $\Gamma$. 现在由此证明自然数系 $N$ 的 Hilbert 第 10 问题也递归可解，从而与已知结果矛盾.

任给一个整系数不定方程：

$$p(n_1,\cdots,n_m)=0 \tag{1}$$

根据 $p$, 我们能行地写出下列整系数不定方程:

$$\sum_{j=1}^{m} P_1(n_j, k_{1j}, \cdots, k_{4j}, t_{1j}, x_{1j}, \cdots, s_{1j}, \cdots, t_{4j}, x_{4j}, \cdots, s_{4j}) + (p(n_1, \cdots, n_m))^2 = 0. \tag{2}$$

(I) 若 (1) 在 $\mathbf{N}$ 中有解, 则由定理 1 易知 (2) 在 $R(\sqrt{D})$ 中有解.

(II) 反之, 若 (2) 在 $R(\sqrt{D})$ 中有解, 则由 (2) 左端形状及 $P_1$ 的构成 (为平方和) 易知有

$$P_1(n_j, k_{1j}, \cdots, k_{4j}, t_{1j}, x_{1j}, \cdots, s_{1j}, \cdots, t_{4j}, x_{4j}, \cdots, s_{4j}) = 0$$

$(j = 1, \cdots, m)$, 故由定理 1 知 $n_1, \cdots, n_m \in \mathbf{N}$, 再由 (2) 即知 (1) 在 $\mathbf{N}$ 中有解.

(III) 由 (I) 及 (II) 可知: 只须用 $\Gamma$ 判定 (2) 在 $R(\sqrt{D})$ 中是否有解, 即可判定 (1) 在 $\mathbf{N}$ 中是否有解. 这与已知结果矛盾.

## § 2 虚二次数环的情况

在本节中, 设整数 $D \leqslant -1$ 无平方因子. 以 $R(\sqrt{D})$ 记数域 $\mathbf{Q}(\sqrt{D})$ 中全体代数整数所成的二次数环.

为了讨论 $R(\sqrt{D})$, 我们先考虑数域 $\mathbf{Q}(\sqrt{D}, \sqrt{F})$ (其中整数 $F > 1$ 且无平方因子) 中全体代数整数所成的双二次数环 $R(\sqrt{D}, \sqrt{F})$. 在这类数环中, 仅有的 1 的单位根是: $\pm 1, \pm \mathrm{i}, (\pm 1 \pm \sqrt{3}\mathrm{i})/2, (\pm\sqrt{2} \pm \sqrt{2}\mathrm{i})/2, (\pm\sqrt{3} \pm \mathrm{i})/2$ (参看本节末注 1).

以 $\sigma_1, \sigma_2$ 各记 $R(\sqrt{D}, \sqrt{F})$ 的如下决定的自同构:

$$\sigma_1(\sqrt{F}) = -\sqrt{F}, \quad \sigma_1(\sqrt{D}) = \sqrt{D};$$
$$\sigma_2(\sqrt{F}) = \sqrt{F}, \quad \sigma_2(\sqrt{D}) = -\sqrt{D}.$$

由 Dirichlet–Minkowski 单位定理知：在 $R(\sqrt{D}, \sqrt{F})$ 中存在 1 个基本单位 $\eta$(它不是 1 的单位根), 使 $R(\sqrt{D}, \sqrt{F})$ 中每一单位 $u$ 都能唯一地表示为 $u = \rho\eta^m$ $(m \in \mathbf{Z})$ 形状，其中 $\rho$ 是 $R(\sqrt{D}, \sqrt{F})$ 中 1 的单位根．(参看本节末注 2)．由同一定理又知：在实二次数环 $R(\sqrt{F})$ 中存在 1 个基本单位 $\varepsilon$(不是 1 的单位根), 使 $R(\sqrt{F})$ 中每一单位 $e$ 都能唯一地表示为 $e = \pm\varepsilon^l$ $(l \in Z)$ 形状.

显然 $\varepsilon$ 也是 $R(\sqrt{D}, \sqrt{F})$ 中的单位，故可表为 $\varepsilon = \rho\eta^m$, 从而有

$$\varepsilon \cdot \sigma_2(\varepsilon) = (\rho\eta^m) \cdot \sigma_2(\rho\eta^m) = (\rho \cdot \sigma_2(\rho))(\eta \cdot \sigma_2(\eta))^m.$$

由 $\sigma_2$ 定义知：$\sigma_2(\varepsilon) = \varepsilon$; $\rho \cdot \sigma_2(\rho) \in R(\sqrt{F})$ 且仍为 1 的单位根，故为 $\pm1$; $\eta \cdot \sigma_2(\eta) \in R(\sqrt{F})$ 且仍为一单位 $e$. 所以上式又可记为

$$\varepsilon^2 = \pm\varepsilon^{lm}.$$

由此式有 $|\varepsilon|^2 = |\varepsilon|^{lm}$, 又由 $\varepsilon \neq \pm1$ 及 $R(\sqrt{F})$ 为实知 $|\varepsilon| \neq 1$, 所以 $|m|$ 为 1 或 2. 再由 $\varepsilon = \rho\eta^m$ 即易得

$$\eta^2 = \rho_1\varepsilon^j. \tag{1}$$

其中 $j = \pm1$ 或 $\pm2$, $\rho_1$ 为 $R(\sqrt{D}, \sqrt{F})$ 中 1 的一个单位根.

**引理 7** 设 $A = 2$, $F = A^2 - 1 = 3$ (当 $D \neq -1$ 且 $D \neq -3$ 时) 或 $A = 4$, $F = A^2 - 1 = 15$ (当 $D = -1$ 或 $-3$ 时). 若 $x, y \in R(\sqrt{D})$ 适合 $x^2 - Fy^2 = 1$, 则 $y^2 \in Z$.

**证明** 由题设有 $(x + \sqrt{F}y)(x - \sqrt{F}y) = 1$, 所以 $x + \sqrt{F}y$ 是 $R(\sqrt{D}, \sqrt{F})$ 中的单位，可以表示为 $x + \sqrt{F}y = \rho\eta^m$, 从而 $x - \sqrt{F}y = \rho^{-1}\eta^{-m}$. 此二式相减再平方，可得

$$4Fy^2 + 2 = \rho^2\eta^{2m} + \rho^{-2}\eta^{-2m}.$$

再将 (1) 代入，得

$$4Fy^2 + 2 = \rho^2\rho_1^m\varepsilon^{jm} + \rho^{-2}\rho_1^{-m}\varepsilon^{-jm}.$$

令 $\lambda=\rho^2\rho_1^m$, $n=jm$, 则上式可记为

$$4Fy^2+2=\lambda\varepsilon^n+\lambda^{-1}\varepsilon^{-n}. \tag{2}$$

其中 $\lambda$ 为 $R(\sqrt{D},\sqrt{F})$ 中一个 1 的单位根.

对于题设中的 $F=3$ 或 15 而言, $R(\sqrt{F})$ 中的单位 $\varepsilon$ 适合 $N(\varepsilon)=1$. (因: 由 $\varepsilon$ 为单位知 $N(\varepsilon)=\pm1$. 又由 $F\equiv3(\bmod 4)$ 知 $\varepsilon$ 可表为 $a+b\sqrt{F}$ $(a,b\in\mathbf{Z})$ 形状, 所以 $N(\varepsilon)=a^2-Fb^2\equiv a^2(\bmod 3)$. 由于 $-1$ 不是 3 的平方剩余, 所以 $N(\varepsilon)\neq-1$). 所以 $\varepsilon^{-1}=\bar{\varepsilon}=\sigma_1(\varepsilon)$. 从而由 (2) 又有

$$4Fy^2+2=\lambda\varepsilon^n+\lambda^{-1}\sigma_1(\varepsilon^n). \tag{3}$$

现在计算 (3) 式两端的虚数部分. 由 $\varepsilon\in R(\sqrt{F})$ 知 $\varepsilon^n$ 及 $\sigma_1(\varepsilon^n)$ 为实数, 由 $\lambda$ 为 1 的单位根知 $\mathrm{Im}(\lambda^{-1})=-\mathrm{Im}(\lambda)$ (Im 表示虚数部分), 故有

$$\begin{aligned}\mathrm{Im}(4Fy^2+2)&=\varepsilon^n\mathrm{Im}(\lambda)+\sigma_1(\varepsilon^n)\mathrm{Im}(\lambda^{-1})\\&=(\varepsilon^n-\sigma_1(\varepsilon^n))\mathrm{Im}(\lambda)\end{aligned} \tag{4}$$

又由于 $y\in R(\sqrt{D})$ 而 $\varepsilon\in R(\sqrt{F})$, 故有

$$\mathrm{Im}(4Fy^2+2)=q_1\sqrt{|D|},\quad (q_1\in\mathbf{Q})$$

及

$$\varepsilon^n-\sigma_1(\varepsilon^n)=q_2\sqrt{F},\quad (q_2\in\mathbf{Q}).$$

又由本节开始时所述关于 1 的单位根情况可知

$$\mathrm{Im}(\lambda)=q_3\sqrt{S},\quad (q_3\in\mathbf{Q};\quad S=0,1\text{ 或 }3.)$$

(由 $F=3$ 或 15 可知 $S\neq2$.) 所以由 (4) 可得

$$q_1\sqrt{|D|}=q_2q_3\sqrt{F}\sqrt{S}.$$

再由题设中 $F$ 与 $D$ 的关系易知,此式两端只能是 0, 所以 $\mathrm{Im}(4Fy^2+2)=0$. 从而有 $4Fy^2+2\in\mathbf{Q}$ 及 $y^2\in\mathbf{Q}$. 再由 $y$ 为代数整数即知 $y^2\in\mathbf{Z}$.  (证毕)

**引理 8** 设 $W,S\in\mathbf{Z}$; $t\in R(\sqrt{D})$ 并且 $N(t)<\dfrac{W^2}{4}$. 若在 $R(\sqrt{D})$ 中有 $S\equiv t(\mathrm{mod}\, W)$, 则 $t\in\mathbf{Z}$.

**证明** 由题设有

$$t=S+W\Big(\frac{U+V\sqrt{|D|}i}{2}\Big),\quad (U,V\in\mathbf{Z}),$$

从而

$$N(t)=\Big(S+\frac{UW}{2}\Big)^2+|D|\frac{V^2W^2}{4}.$$

若 $V\neq 0$, 则易见 $N(t)\geqslant\dfrac{W^2}{4}$, 与题设不合. 所以 $V=0, t\in\mathbf{Q}$. 又因 $t\in R(\sqrt{D})$, 所以 $t\in\mathbf{Z}$.  (证毕)

**引理 9** 依引理 7 的题设取自然数 $F$. 令 $\Sigma$ 为下列不定方程组 (以 $t,x,y,u,v,z,w,h,r,s$ 为未知数):

$$\Sigma\begin{cases}\text{(a)}\ \ x^2-Fy^2-1=0,\\ \text{(b)}\ \ u^2-Fv^2-1=0,\\ \text{(c)}\ \ v^2-y^2t-zy^4=0,\\ \text{(d)}\ \ ry+s(5h+2)-1=0,\\ \text{(e)}\ \ y-2tw=0.\end{cases}$$

则有下列二结论成立:

(i) 若 $\Sigma$ 在 $R(\sqrt{D})$ 中有解为 $\langle t,x,\cdots,s\rangle$, 则 $t\in\mathbf{Z}$.

(ii) 若 $k\neq 0$ 为一自然数, 则 $\Sigma$ 在 $R(\sqrt{D})$ 中有一组解 $\langle t,x,\cdots,s\rangle$ 其 $t=k^2$.

**证明** (I) 先证 (i). 已知 $t,x,\cdots,s\in R(\sqrt{D})$ 适合 $\Sigma$.

假若 $y=0$, 则由 (d) 有 $s(5h+2)=1$, 从而 $5h+2$ 为单位. 但易知虚二次数环中的单位只有 $\pm1,\pm\mathrm{i}$ 及 $(\pm1\pm\sqrt{3}\mathrm{i})/2$. 再由 $h\in R(\sqrt{D})$ 即易得矛盾. 所以 $y\neq 0$.

由 (a),(b) 及引理 7 知 $y^2 \in \mathbf{Z}$ 且 $v^2 \in \mathbf{Z}$. 由 (c) 知在 $R(\sqrt{D})$ 中 $y^2|v^2$ 且

$$(v^2/y^2) \equiv t \pmod{y^2} \tag{1}$$

由 (e) 知

$$N(y^2) = 16(N(t))^2(N(w))^2.$$

再由 $y \neq 0$ 知 $t \neq 0$ 且 $w \neq 0$, 从而有 $(N(w))^2 \geqslant 1$ 及 $(N(t))^2 \geqslant 1$, 由此又易知

$$N(y^2) \geqslant 16(N(t))^2 > 4N(t).$$

但由 $y^2 \in \mathbf{Z}$ 知 $N(y^2) = y^4$, 故得

$$N(t) < y^4/4 \tag{2}$$

由以上又易见 $v^2/y^2 \in \mathbf{Z}$. 再由 (1),(2) 及引理 8 即得 $t \in \mathbf{Z}$.

(II) 再证 (ii). 已知 $k \neq 0$ 为一自然数. 令 $t = k^2$, 则 $F(2t)^2$ 非平方数, 故由引理 1 知存在 $X, Y \in \mathbf{N}$ 适合 $Y \neq 0$ 及

$$X^2 - F(2t)^2Y^2 = 1.$$

但 $F = A^2 - 1$, 故由引理 2 知存在自然数足码 $n$ 使 $X = X_n(A)$ 及 $2tY = Y_n(A)$. 现在令

$$x = X_n(A),\ y = Y_n(A),\ u = X_{nk}(A),\ v = Y_{nk}(A),\ w = Y.$$

则 (e) 显然适合, 并且 $y \neq 0$ (因 $t \neq 0$ 且 $w \neq 0$). 由引理 2, (a) 及 (b) 也适合. 由引理 3, 存在 $z \in R(\sqrt{D})$ 使 (c) 适合. 由于 $y \neq 0$, 又可以取得一自然数 $h$ 使 $5h+2$ 与 $y$ 在 $\mathbf{N}$ 中无公因子 (因: 由 Dirichlet 定理知, 当 $h$ 通过 $\mathbf{N}$ 时, 在 $5h+2$ 中有无限多个 $\mathbf{N}$ 中的素数). 从而又存在 $r, s \in \mathbf{Z}$ 使 (d) 适合. (证毕)

把 $\Sigma$ 中 (a) 至 (e) 左端的多项式各记为 $p_1(t,x,\cdots,s),\cdots,$ $p_5(t,x,\cdots,s)$. 并以 $\prod(n,t_1,x_1,\cdots,s_1,k_1,\cdots,t_4,x_4,\cdots,s_4,k_4)$ 记下列谓词:

$$\{n=0\}\vee\left\{_1\bigwedge_{i=1}^{5}[p_i(t_1,x_1,\cdots,s_1)=0]\wedge[t_1-k_1^2=0]\right.$$

$$\left.\wedge[(n-k_1^2)(n+k_1^2)=0]\right\}_1$$

$$\vee\left\{_2\bigwedge_{j=1}^{2}\left\{\bigwedge_{i=1}^{5}[p_i(t_j,x_j,\cdots,s_j)=0]\wedge[t_j-k_j^2=0]\right\}\right.$$

$$\left.\wedge[(n-k_1^2-k_2^2)(n+k_1^2+k_2^2)=0]\right\}_2$$

$$\vee\cdots\vee\left\{_4\bigwedge_{j=1}^{4}\left\{\bigwedge_{i=1}^{5}[p_i(t_j,x_j,\cdots,s_j)=0]\wedge[t_j-k_j^2=0]\right\}\right.$$

$$\left.\wedge[(n-k_1^2-k_2^2-k_3^2-k_4^2)(n+k_1^2+k_2^2+k_3^2+k_4^2)=0]\right\}_4.$$

由引理 9 易见，对任何 $n\in R(\sqrt{D})$ 都有: “$n\in\mathbf{Z}$” 当且只当“谓词 $(\exists\, t_1,\cdots,k_1,\cdots,t_4,\cdots,k_4)\prod(n,t_1,\cdots,k_1,\cdots,t_4,\cdots,k_4)$ 在 $R(\sqrt{D})$ 中成立.”

把上述的谓词 $(\exists\, t_1,\cdots,k_4)\prod(n,t_1,\cdots,k_4)$ 简记为 $\Gamma(n)$, 再令谓词 $\Gamma_1(m)$ 为:

$$(\exists n_1\cdots n_4)[\Gamma(n_1)\wedge\cdots\wedge\Gamma(n_4)\wedge(m-n_1^2-n_2^2-n_3^2-n_4^2=0)],$$

则易见对任何 $m\in R(\sqrt{D})$ 都有: “$m\in\mathbf{N}$” 当且只当 “$\Gamma_1(m)$ 在 $R(\sqrt{D})$ 中成立”.

有了以上的讨论之后，我们还要设法把上述的谓词 $\Gamma_1(m)$ 用一个整系数不定方程来表示. 为此，我们任意取定一个无平方因子且不等于 0,1,$D$ 的整数 $D'$. 不难看出，对于 $R(\sqrt{D})$ 中任二数 $x,y$

都有

$$\text{“}x=0 \text{ 且 } y=0\text{” 当且只当 “}x^2-D'y^2=0\text{”}, \tag{1}$$

以及

$$\text{“}x=0 \text{ 或 } y=0\text{” 当且只当 “}xy=0\text{”}. \tag{2}$$

反复利用 (1) 及 (2), 易见可以把 $\Gamma_1(m)$ 改写成一个在 $R(\sqrt{D})$ 中与之等价的如下形状的谓词:

$$(\exists\, n_1\cdots n_4 t_1\cdots k_1\cdots t_4\cdots k_4)[P_1(m,n_1,\cdots,n_4,\\ t_1,\cdots,k_1,\cdots,t_4,\cdots,k_4)=0],$$

其中 $P_1$ 是一个特定的整系数多项式.

由以上讨论, 即见有下列定理成立:

**定理 3** 设 $m\in R(\sqrt{D}),(D\leqslant -1)$, 则 $m\in \mathbf{N}$ 的充分必要条件是: 对于上述特定的整系数多项式 $P_1$ 而言, 存在 $n_1,\cdots,n_4,t_1,\cdots,k_1,\cdots,t_4,\cdots,k_4\in R(\sqrt{D})$ 使

$$P_1(m,n_1,\cdots,n_4,t_1,\cdots,k_1,\cdots,t_4,\cdots,k_4)=0.$$

在此基础上, 又可进一步得到

**定理 4** 设 $R(\sqrt{D})$ 为任一虚二次数环, 则 $R(\sqrt{D})$ 中的 Hilbert 第 10 问题递归不可解.

**证明** 仿定理 2 的证明思路. 只须用上述的 (1) 代替实二次数环时的平方和来处理方程的合取, 并用定理 3 代替定理 1 即可. (证毕)

**注 1** 由代数数论知, $m$ 次分圆域 $\mathbf{Q}(\rho)$ 在 $\mathbf{Q}$ 上的次数为 $\varphi(m)$ ($\varphi$ 为 Euler 函数). 并且易见适合 $\varphi(m)\leqslant 4$ 的 $m$ 只有: 1,2,3,4,5,6,8,10,12. 在这些 $m$ 中, 除 $m=5,10$ 者外, 易知 1 的 $m$ 次单位根已如上面所列举. 而 1 的 5 次或 10 次单位根不会被包含在任一个双二次域 $\mathbf{Q}(\sqrt{D},\sqrt{F})$ 中, 理由如下: 设 $\rho\neq 1$ 为 1 的一

个 5 次单位根，则 $\rho$ 适合方程 $g(x)=x^4+x^3+x^2+x+1=0$. 习知 $g(x)$ 在 $\mathbf{Q}$ 上不可约，所以 $\mathbf{Q}(\rho)$ 是 $\mathbf{Q}$ 的 4 次扩域. 考虑 $\mathbf{Q}(\rho)$ 的由 $\rho\longrightarrow\rho^2$ 所决定的自同构 $\theta$, 易知 $\theta$ 的周期为 4. 另一方面，对任何双二次域 $\mathbf{Q}(\sqrt{D},\sqrt{F})$, 易知它没有周期为 4 的自同构. 所以 $\mathbf{Q}(\rho)\neq\mathbf{Q}(\sqrt{D},\sqrt{F})$, 从而易知 $\rho\notin\mathbf{Q}(\sqrt{D},\sqrt{F})$. 又设 $\lambda\neq\pm1$ 为 1 的一个 10 次单位根，则由 $0=\lambda^{10}-1=(\lambda^5-1)(\lambda^5+1)$ 知 $\lambda$ 为 $\pm\rho$ 形状，其中 $\rho\neq1$ 为 1 的 5 次单位根. 所以也有 $\mathbf{Q}(\lambda)=\mathbf{Q}(\rho)\neq\mathbf{Q}(\sqrt{D},\sqrt{F})$, 从面易知 $\lambda\notin\mathbf{Q}(\sqrt{D},\sqrt{F})$.

**注 2** Dirichlet–Minkowski 单位定理是说：设 $\mathbf{Q}(\alpha)$ 为一 $n$ 次代数数域，$R(\alpha)$ 为其代数整数环. 若在 $\alpha$ 的 $n$ 个共轭根 (包括 $\alpha$ 自身) 中有 $r_1$ 个实根，$r_2$ 对共轭复根，令 $r=r_1+r_2-1$, 则在 $R(\alpha)$ 中存在 $r$ 个基本单位 $\eta_1,\cdots,\eta_r$, 使 $R(\alpha)$ 中每一单位 $u$ 都能唯一地表示为如下形状：

$$u=\rho\eta_1^{m_1}\cdots\eta_r^{m_r}.$$

其中 $m_1,\cdots,m_r\in\mathbf{Z}$ 面 $\rho$ 为 $R(\alpha)$ 中 1 的一个单位根. 对于我们所讨论的域 $\mathbf{Q}(\sqrt{D},\sqrt{F})$ 来说，当把它表示为 $\mathbf{Q}(\alpha)$ 形状后，由 $D\leqslant-1$ 及 $F>1$ 易知 $\alpha$ 所适合的 $\mathbf{Q}$ 上 4 次多项式有 2 对共轭复根，所以这时 $R(\alpha)=R(\sqrt{D},\sqrt{F})$ 中基本单位的个数为 $r=0+2-1=1$.

## 参考文献


1 Davis M. Hilbert's tenth problem is unsolvable. Amer. Math. Monthly, 1973, 80: 233~269

2 胡久稔. 希尔伯特第十问题. 沈阳: 辽宁教育出版社, 1987

3 Pheidas Th. Extensions of Hilbert's tenth problem. Jour. Symbolic Logic, 1994, 59: 372~397

4 Denef J. Hilbert's tenth problem for quadratic rings. Proc. Amer. Math. Soc., 1975, 48: 214~220

# 第 4 章

# 某些环的 Goldbach 性质

Goldbach 猜想是数论中的著名难题，其研究主要是用解析数论方法. 本章的内容与前人关于 Goldbach 猜想的研究关系不大，是要用数理逻辑中的模型论方法讨论某些可换环中与 Goldbach 猜想类似的性质. 在 § 1 中，我们在前人解析数论成果基础上用模型论方法证明：存在某些无限域 $F$, 其上的多项式环 $F[x]$ 能适合 Goldbach 3 素元性质. 在 § 2 及 § 3 中，我们根据二次代数整数环的一些简单性质用模型论方法证明：对每个二次数环 $R$, 都存在其扩环能适合与 Goldbach 猜想类似的性质，也存在其扩环不适合这种性质. 这两者结合起来，说明了 Goldbach 性质对于与 $R$ 相关的某种较弱理论 (指：由 $R$ 的上述两种扩环的公共性质所构成的命题集) 的独立性. 这种独立性也在一定程度上反映了在整数环中 (或在 $R$ 中) 研究 Goldbach 猜想的难度.

## § 1 某些无限域上多项式环的 Goldbach 3 素元性质

1991 年， E. W. Effinger 和 D. R. Hayes 在其解析数论专著

[1] 及有关文献的基础上，经过计算机辅助计算，证明了关于有限域上 1 元多项式环的一种 Goldbach 3 素元性质 (可参看 [2]), 其主要内容如下：

**定理 1** (以下称 EH 定理) (i) 设 $F$ 为任一元数为奇数的有限域， $F[x]$ 为 $F$ 上 1 元多项式环，则 $F[x]$ 中每个次数 $d \geqslant 2$ 且首系数为 1 的多项式都可表示为 3 个首系数为 1 的不可约多项式之和，其中 1 个次数为 $d$, 另 2 个次数较低． (ii) 设 $F$ 为任一元数为偶数的有限域，则 $F[x]$ 中每个次数 $d \geqslant 3$ 且首系数为 1 的多项式也可类似地表示为 3 个首系数为 1 的不可约多项式之和．

这个定理，是数论中已被 I. M. Vinogradov 等对充分大的奇数证明了的 Goldbach 3 素数猜想 (即：每个 $\geqslant 7$ 的奇数都可表示为 3 个素数之和) 的一种类似物．这种 3 素元性质，在 $F$ 为无限域时未必成立．例如当 $F$ 为代数闭域或实闭域时， $F[x]$ 中不可约多项式都是 1 次或 2 次的， 3 素元性质显然不能成立．在本节中，我们要引用模型论方法来证明由 EH 定理可得如下结论：存在着无限多个无限域 $F$, 与之相应的 $F[x]$ 有 3 素元性质成立 (见以下定理 2 至定理 4)．本节的这些结论，其证明只用到 EH 定理的陈述本身及模型论中两个定理，而不需用解析数论方法或计算机的计算． (事实上，本节内容也不依赖于 EH 定理的由计算机支持的部分，由 [2] 及下面的证法可以看出．)

**定理 2** 存在无限多个特征数为 0 的归纳域 $F$, 使 $F[x]$ 中每个次数 $d \geqslant 2$ 且首系数为 1 的多项式都可表示为 3 个首系数为 1 的不可约多项式之和，其中 1 个次数为 $d$, 另 2 个次数较低．

**证明** 令形式语言 $\mathcal{L} = \{0, 1, \xi, +, \cdot, C\}$, 其中 $0, 1, \xi$ 为个体常量符号； $+, \cdot$ 为 2 元运算符号； $C$ 为 1 元关系符号．

(I) 现在定义 $\mathcal{L}$ 上的 1 阶理论 $T_0 = A_1 \cup A_2 \cup \cdots \cup A_6$; 其中诸 $A_i$ 是 $\mathcal{L}$ 上如下的 1 阶语句组：

$A_1$ 是由 $+, \cdot$ 表述的可换环公理组，以 0 为零元， 1 为乘法单

位元.

$A_2$ 表述: 适合 $C$ 的元构成一个子域 (以下简称为 $C$ 域). 它包括下列诸语句:

$$C(0) \wedge C(1),$$
$$\forall xy[(C(x) \wedge C(y) \rightarrow (C(x+y) \wedge C(x \cdot y))],$$
$$\forall x[C(x) \rightarrow \exists y(C(y) \wedge x + y = 0)],$$
$$\forall x[(C(x) \wedge x \neq 0) \rightarrow \exists y(C(y) \wedge x \cdot y = 1)].$$

$A_3$ 表述: $C$ 域的特征数为 0. 它包括下列无限多个语句:

$$1 + 1 \neq 0, \quad 1 + 1 + 1 \neq 0, \cdots$$

$A_4$ 表述: $C$ 域是归纳域, 即适合 1 阶归纳原理. 它包括 $\mathcal{L}$ 上一切如下形状的 1 阶语句:

$$[\varphi(0) \wedge \forall x((C(x) \wedge \varphi(x)) \rightarrow \varphi(x+1))] \rightarrow \forall x[C(x) \rightarrow \varphi(x)].$$

其中 $\varphi(x)$ 通过 $\mathcal{L}$ 上一切只含自由变元 $x$ 并且约束变元都已对 $C$ 相对化了的公式. (关于归纳域, 可参看 [3] 或 [4].)

$A_5$ 表述: $\xi$ 是 $C$ 域上的超越元. 它包括下列无限多个语句:

$$\forall x[C(x) \rightarrow (\xi + x \neq 0)],$$
$$\forall xy[(C(x) \wedge C(y)) \rightarrow (\xi^2 + x\xi + y \neq 0)],$$
$$\forall xyz[(C(x) \wedge C(y) \wedge C(z)) \rightarrow (\xi^3 + x\xi^2 + y\xi + z \neq 0)],$$
$$\cdots\cdots$$

$A_6$ 表述 $C$ 域上 $\xi$ 的多项式的 3 素元性质. 它包括无限多个

语句 $\varphi_2, \varphi_3, \varphi_4, \cdots$. 例如 $\varphi_2$ 为

$$\forall xy[(C(x) \wedge C(y)) \to \exists u_1 v_1 u_2 u_3 [C(u_1) \wedge C(v_1) \wedge C(u_2) \wedge C(u_3)$$
$$\wedge (\xi^2 + x\xi + y = (\xi^2 + u_1\xi + v_1) + (\xi + u_2) + (\xi + u_3))$$
$$\wedge \neg \exists w_1 w_2 [C(w_1) \wedge C(w_2) \wedge (\xi^2 + u_1\xi + v_1 = (\xi + w_1)(\xi + w_2))]]],$$

$\varphi_3$ 为 (用示意性简写)

> $\forall xyz[(C(x) \wedge C(y) \wedge C(z)) \to \exists u_1 v_1 w_1 u_2 v_2 u_3 v_3\ [C(u_1) \wedge \cdots \wedge C(v_3) \wedge [(\xi^3 + x\xi^2 + y\xi + z$ 为 $\xi^3 + u_1\xi^2 + v_1\xi + w_1$ 与 $\xi^2 + u_2\xi + v_2$ 与 $\xi^2 + u_3\xi + v_3$ 之和且后 3 者在 $C$ 域上都不可约$) \vee (\xi^3 + x\xi^2 + y\xi + z$ 为 $\xi^3 + u_1\xi^2 + v_1\xi + w_1$ 与 $\xi^2 + u_2\xi + v_2$ 与 $\xi + u_3$ 之和且后 3 者在 $C$ 域上都不可约$) \vee (\xi^3 + x\xi^2 + y\xi + z$ 为 $\xi^3 + u_1\xi^2 + v_1\xi + w_1$ 与 $\xi + u_2$ 与 $\xi + u_3$ 之和且后 3 者在 $C$ 域上都不可约$)]]]$,

等等.

(II) 现在证明 $T_0$ 有模型. 任取 $T_0$ 的有限子集 $S$, 则 $S$ 只含 $A_3$ 中有限多个语句, 设这些语句中在左端最多出现 $q$ 个 1. 任取一奇素数 $p > q$, 则由 EH 定理可知 $p$ 元域 $F_p$ 上的多项式环 $F_p[x]$ 就能适合 $S$ 中一切语句 (以 $F_p$ 中的元作为适合 $C$ 的元, 以 $x$ 作为 $\xi$ 的解释), 所以 $S$ 有模型. 再由有限子集 $S$ 的任意性及紧致性定理 (可参看 [5] 定理 1.3.22) 即知 $T_0$ 自身有模型.

(III) 任取 $T_0$ 的模型 $M$, 设其中对 $\xi$ 的解释为 $\alpha$. 由 $T_0$ 的 $A_1$ 至 $A_4$ 中诸语句可知 $M$ 为一可换环, 其中适合 $C$ 的元素构成 $M$ 的一个特征数为 0 的子域 $F$, 它是归纳域. 由 $A_5$ 知 $\alpha$ 是 $F$ 上的超越元, 从而 $M$ 的子环 $F[\alpha]$ 就是 $F$ 上的 1 元多项式环, 再由 $A_6$ 可知 $F[\alpha]$ 适合 3 素元性质.

(IV) 设上述的 $M$ 基数为 $\gamma$, 其 $C$ 域 $F$ 的基数为 $\delta$, 则 $M$ 是 $T_0$ 的 $(\gamma, \delta)$ 模型且 $\delta$ 为无限基数. 从而由双基数 LS 定理 (参看 [5]

定理 4.3.10) 可知，对任何基数 $\lambda$, $T_0$ 都有基数为 $\gamma^\lambda$ 的模型，其 $C$ 域的基数为 $\delta^\lambda$. 由此即不难看出：存在无限多个基数互异因而互不同构的特征数为 0 的归纳域 $F$, 与之相应的 $F[x]$ 都适合 3 素元性质. (证毕)

以上所说互不同构的诸归纳域，是从基数不同这方面来看的. 如果我们对 $T_0$ 以不同方式增加一些新语句，还可得到各种代数性质明显不同的归纳域 $F$, 其 $F[x]$ 都适合 3 素元性质. 例如：

令 $T_{01} = T_0 \cup \{\exists x(C(x) \wedge x^2 + 1 = 0)\}$, 则可仿上证明 $T_{01}$ 有模型，只需根据整数的平方剩余性质在 (II) 中取 $p$ 为大于 $q$ 并且形状为 $4n+1$ 的素数即可 (由 Dirichlet 定理知 $p$ 存在). 在由 $T_{01}$ 的模型所得的 $C$ 域中， $-1$ 能开平方.

令 $T_{02} = T_0 \cup \{\neg\exists x(C(x) \wedge x^2 + 1 = 0)\}$, 也可仿上证明 $T_{02}$ 有模型，只需在 (II) 中取 $p$ 为大于 $q$ 并且形状为 $4n+3$ 的素数即可. 在由 $T_{02}$ 的模型所得的 $C$ 域中， $-1$ 不能开平方.

又如，若分别令 $T_{03} = T_{01} \cup \{\exists x(C(x) \wedge x^2 - 2 = 0)\}$ 及 $T_{04} = T_{01} \cup \{\neg\exists x(C(x) \wedge x^2 - 2 = 0)\}$, 并且在 (II) 中分别取 $p$ 为大于 $q$ 且形状为 $8n+1$ 或 $8n+5$ 的素数，则可知 $T_{03}$ 及 $T_{04}$ 都有模型. 在由它们分别所得的 $C$ 域中，前者 $-1$ 及 2 都能开平方，而后者 $-1$ 能开平方， 2 不能开平方.

我们也可在 $T_{02}$ 基础上仿上定义 $T_{05}$ 及 $T_{06}$, 使由之所得的 $C$ 域对 $-1$ 不能开平方而对 2 则分别能开平方或不能开平方，为此只需在 (II) 中取 $p$ 为大于 $q$ 且形状分别为 $8n+7$ 或 $8n+3$ 的素数即可. 我们又可在 $T_{03}$ 至 $T_{06}$ 的基础上增加关于其他整数能否开平方的语句，从而得到各种性质不同的 $C$ 域. 如此等等，不再赘述.

**定理 3** 对每个奇素数 $p$, 都存在无限多个特征数为 $p$ 的无限域 $F$, 使 $F[x]$ 适合定理 2 中所说的 3 素元性质.

**证明** 证法与定理 2 的证明类似，只需作如下改变：

对于任意取定的奇素数 $p$, 首先把 $T_0$ 换为 $\mathcal{L}$ 上的 1 阶理论 $T_p = A_1 \cup A_2 \cup \{k_p\} \cup A_5 \cup A_6 \cup A_7$, 其中 $A_1, A_2, A_5, A_6$ 与 $T_0$ 者相同, $k_p$ 为下列语句:

$$1+1+\cdots+1=0 \ \text{(左端为 } p \text{ 个 1 相加)},$$

$A_7$ 表述: 适合 $C$ 的元素有无限多个, 它包括下列无限多个语句:

$$\exists xy[C(x) \wedge C(y) \wedge (x \neq y)],$$
$$\exists xyz[C(x) \wedge C(y) \wedge C(z) \wedge (x \neq y) \wedge (x \neq z) \wedge (y \neq z)],$$
$$\cdots\cdots$$

其次, 在引用紧致性定理证明 $T_p$ 有模型时, 对于 $T_p$ 的任一有限子集 $S$, 设其所含 $A_7$ 中的有限个语句最多是说 "存在 $q$ 个不同的 $C$ 元", 则可取 $p$ 的幂 $p^m \geqslant q$, 再由 EH 定理知 $p^m$ 元域上的 1 元多项式环就能适合 $S$ 中一切语句. 故由 $S$ 的任意性可知 $T_p$ 有模型. (证毕)

**定理 4** 存在无限多个特征数为 2 的无限域 $F$, 使 $F[x]$ 中每个次数 $d \geqslant 3$ 且首系数为 1 的多项式都可表为 3 个首系数为 1 的不可约多项式之和, 其中 1 个次数为 $d$, 另 2 个次数较低.

**证明** 与定理 3 的证法类似, 但在定义 $T_2$ 时需从 $A_6$ 中把 $\varphi_2$ 去掉.

本节内容取材于 [6].

## § 2 二次数环的具有 Goldbach 性质的扩环

令 $\mathbf{Z}$ 为整数环, $m$ 为任一个无平方因子并且适合 $m \equiv 2 \pmod 4$ 或 $m \equiv 3 \pmod 4$ 的有理整数. 考虑二次代数整数环 $\mathbf{Z}[\sqrt{m}]$

$= \{a + b\sqrt{m} \mid a, b \in \mathbf{Z}\}$. 我们将证明：存在 $\mathbf{Z}[\sqrt{m}]$ 的扩环 $R$, $R$ 具有 Goldbach 性质. (指：任何非 0 也非单位的元 $\alpha$ 的 2 倍都是两个素元的和.) 为此，先证明两个引理.

**引理 1** 对于上述的 $m$, 在 $\mathbf{Z}$ 中存在无限多个适合下列性质 $(\Pi_1)$ 的素数 $p$:

$(\Pi_1)$ 对任何 $a, b \in \mathbf{Z}$, 若 $p \nmid a$ 或 $p \nmid b$, 则 $p \nmid a^2 - mb^2$.

**证明** (I) 任取一个不以 $m$ 为平方剩余的素数 $p$ (其存在性见下面 (II)). 今证 $p$ 适合 $(\Pi_1)$:

(1.1) 假若有 $a, b \in \mathbf{Z}$ 使:

$$p \nmid a \text{ 而 } p \mid a^2 - mb^2 \tag{1}$$

由 $p \nmid a$ 及 $p$ 为素数，可知存在 $l \in \mathbf{Z}$ 使 $al \equiv b \pmod{p}$, 从而有 $0 \equiv a^2 - mb^2 \equiv a^2(1 - ml^2) \pmod{p}$, 再由 $p \nmid a$ 即易见有 $m \equiv (ml)^2 \pmod{p}$. 这与 $p$ 的取法不合，所以 (1) 不能成立.

(1.2) 假若有 $a, b \in \mathbf{Z}$ 使 $p \nmid b$ 而 $p \mid a^2 - mb^2$, 仿 (1.1) 可得矛盾.

(II) 对于 $m$, 可以定出，在某一等差数列 $cn + d$($c, d$ 互素) 中的素数 $p$ 都不以 $m$ 为平方剩余. (可参看 [7] 中 p.75 通过特例所说明的一般方法). 再由 Dirichlet 定理可知在数列 $cn + d$ 中有无限多个素数 $p$.

由 (I),(II) 即知引理 1 成立. (证毕)

**引理 2** 设有理素数 $p$ 适合上述性质 $(\Pi_1)$. 以 $K$ 记 $\mathbf{Z}[\sqrt{m}]$ 对于理想子环 $(p^3)$ 的剩余类环. 则 $K$ 具有下列诸性质：(a) $K$ 是有 1(乘法单位元) 的可换环. (b) $K$ 不是整环. (c) $K$ 中存在素元，其个数为 $p^4 - p^2$. (d) $K$ 中存在合元，其个数为 $p^2 - 1$. (e) $K$ 适合 Goldbach 性质.

**证明** (a),(b) 易见. 以下证 (c) 至 (e).

(I) 首先，易见可取下列诸数作为 $K$ 中诸剩余类的代表元：

$$a+b\sqrt{m},\quad (0\leqslant a,b<p^3).$$

所以 $K$ 的元数为 $p^6$.

(II) 现在定出 $K$ 中的单位 (即有逆元的元).

(2.1) 设 $a+b\sqrt{m}$ 是 $K$ 中的单位，则存在 $K$ 中的元 $x+y\sqrt{m}$ 适合

$$(a+b\sqrt{m})(x+y\sqrt{m})=1\quad (\text{在 } K \text{ 中}).$$

易见此等价于 $\mathbf{Z}$ 中的同余式组：

$$ax+mby\equiv 1\ (\operatorname{mod} p^3)\tag{1}$$

$$ay+bx\equiv 0\ (\operatorname{mod} p^3)\tag{2}$$

由 (1) 可知：

$$\text{在 } \mathbf{Z} \text{ 中},\quad p\nmid a \text{ 或 } p\nmid b.\tag{3}$$

(2.2) 反之，若 (3) 成立，则由 ($\text{II}_1$) 知 $p\nmid a^2-mb^2$. 从而易见存在 $s\in\mathbf{Z}$ 能使 $(a^2-mb^2)s\equiv 1\ (\operatorname{mod} p^3)$. 今取 $x,y(0\leqslant x,y<p^3)$ 使适合 $x\equiv as$, $y\equiv -bs$, $(\operatorname{mod} p^3)$, 则有

$$ax+mby\equiv (a^2-mb^2)s\equiv 1\ (\operatorname{mod} p^3).$$

及

$$ay+bx\equiv -abs+abs\equiv 0\ (\operatorname{mod} p^3).$$

所以 (1) 及 (2) 成立，从而 $x+y\sqrt{m}$ 是 $a+b\sqrt{m}$ 在 $K$ 中的逆元.

(2.3) 由上可知， $a+b\sqrt{m}$ 在 $K$ 中为单位当且只当 “$p\nmid a$ 或 $p\nmid b$”. 从而易见 $K$ 中单位的个数是 $p^6-p^4$.

(III) 现在定出 $K$ 中的素元及合元.

(3.1) 先证： $p$ 是 $K$ 中的素元.

任取 $p$ 在 $K$ 中的一个因子分解

$$p=(a+b\sqrt{m})(c+d\sqrt{m})\ (\text{在}\ K\ \text{中}).$$

则在 $\mathbf{Z}$ 中有

$$p\equiv ac+mbd\ (\operatorname{mod} p^3) \tag{4}$$

假若 $a+b\sqrt{m}$ 及 $c+d\sqrt{m}$ 都不是 $K$ 中的单位，则由 (2.3) 知在 $\mathbf{Z}$ 中有 $p|a,b,c,d$, 从而有 $p^2|ac+mbd$. 此与 (4) 不合.

所以，$p$ 在 $K$ 中的任何因子分解中至少有一个因子是单位. 又由 (2.3) 知 $p$ 不是 $K$ 中的单位，从而 $p$ 是 $K$ 中的素元.

(3.2) 现在考虑 $K$ 中的素元 $p$ 与任一单位元 $a+b\sqrt{m}$(其中 $0\leqslant a,b<p^2$ 并且 $p\nmid a$ 或 $p\nmid b$) 的乘积. 易见这些乘积 $p(a+b\sqrt{m})$ 在 $K$ 中互不相等，其个数为 $p^4-p^2$.

事实上，这些乘积也都是 $K$ 中的素元. 但由于我们尚不知 $K$ 中是否具有素分解的唯一性，所以不能由上段直接肯定此事. 以下仿照 (3.1) 来证明每个这样的乘积 $p(a+b\sqrt{m})$ 都是 $K$ 中的素元.

任取 $p(a+b\sqrt{m})$ 在 $K$ 中的一个因子分解

$$p(a+b\sqrt{m})=(c+d\sqrt{m})(e+f\sqrt{m})\ (\text{在}\ K\ \text{中}).$$

即：

$$pa+pb\sqrt{m}=(ce+dfm)+(cf+de)\sqrt{m}\ (\text{在}\ K\ \text{中}).$$

所以在 $\mathbf{Z}[\sqrt{m}]$ 中有

$$(pa-ce-dfm)+(pb-cf-de)\sqrt{m}=p^3(u+v\sqrt{m}),$$

从而在 $\mathbf{Z}$ 中有

$$pa-ce-dfm=p^3u \tag{5}$$

$$pb-cf-de=p^3v \tag{6}$$

假若 $c+d\sqrt{m}$ 与 $e+f\sqrt{m}$ 均非 $K$ 中的单位，则由 (2.3) 知 $p|c,d,e,f$. 再由 (5) 及 (6) 可知 $p|a$ 且 $p|b$. 从而 $a+b\sqrt{m}$ 不能是 $K$ 中的单位，与以上矛盾.

所以 $p(a+b\sqrt{m})$ 在 $K$ 中没有真分解，又由 (2.3) 知它不是单位，从而是 $K$ 中的素元.

(3.3) 由 (3.1) 及 (II) 又易知： $p^2$ 是 $K$ 中的合元. 从而又可知，一切形状为 $p^2(a+b\sqrt{m})$ 的元，其中 $0 \leqslant a,b < p$ 并且 $a,b$ 不全为 0 者，都是 $K$ 中与 $p^2$ 相伴的合元 (共有 $p^2-1$ 个).

(3.4) 由 (2.3) 及 (3.2), (3.3) 中关于各种元数的结论可知：(3.2) 中包括了 $K$ 的全部素元. (3.3) 中包括了 $K$ 的全部合元.

(IV) 现在证明 $K$ 适合 Goldbach 性质.

任取 $K$ 中一个非 0 且非单位的元 $\alpha$.

若 $\alpha$ 为素元，则 $2\alpha$ 显然为二素元之和.

若 $\alpha$ 为合元. 则由 (3.3) 及 (3.4) 知 $\alpha$ 为

$$p^2a+p^2b\sqrt{m}\ (0 \leqslant a,b < p)$$

形状，故有

$$2\alpha = (p(pa+1)+p^2b\sqrt{m})+(p(pa-1)+p^2b\sqrt{m}).$$

令

$$\pi_1 = p(pa+1)+p^2b\sqrt{m},$$
$$\pi_2 = p(pa-1)+p^2b\sqrt{m}.$$

(必要时将 $p(pa+1)$ 或 $p(pa-1)$ 换为其对于模 $p^3$ 的最小非负剩余，显见不影响讨论). 则由 (3.2) 可知 $\pi_1,\pi_2$ 都是 $K$ 中的素元.

由以上讨论即知 (c),(d),(e) 成立. (证毕)

**定理 5** 对任何形状为 $\mathbf{Z}[\sqrt{m}]=\{a+b\sqrt{m}|\ a,b\in\mathbf{Z}\}$ 的二次代数整数环 (其中 $m$ 是无平方因子且适合 $m\equiv 2\ (\mathrm{mod}\,4)$ 或

$m \equiv 3 \pmod 4$ 的有理整数), 都存在具有下列诸性质的扩环 $R$: (a) $R$ 是有 1 的可换环. (b) $R$ 不是整环. (c) $R$ 中有无限多个素元. (d) $R$ 中有无限多个合元. (e) $R$ 适合 Goldbach 性质.

**证明** 令语言 $\mathcal{L} = \{+, \cdot, 0, 1, \rho\}$. 令 $T$ 为 $\mathcal{L}$ 上如下的 1 阶理论 (以下用普通语言描述其公理):

$$T \begin{cases} \text{可换环公理, 且以 1 为乘法单位元;} \\ \text{存在零因子;} \\ \text{存在 } n \text{ 个不同的素元}(n = 1, 2, 3, \cdots); \\ \text{存在 } n \text{ 个不同的合元}(n = 1, 2, 3, \cdots); \\ \text{Goldbach 性质;} \\ \mathbf{Z}[\sqrt{m}] \text{的图象.} \end{cases}$$

(其中 $\mathbf{Z}[\sqrt{m}]$ 的图象包括: 此环的加法表, 乘法表及一切不等式 $a + b\sqrt{m} \neq 0$ ($a, b \in \mathbf{Z}$; $a, b$ 不同时为 0). 但在记号上用 $\rho$ 代替 $\sqrt{m}$.)

任取 $T$ 的有限子集 $S$, 则由引理 1 及引理 2 易知能找到足够大的正有理素数 $p$ 使 $\mathbf{Z}[\sqrt{m}]$ 对于理想子环 $(p^3)$ 的剩余类环 $K$ 适合 $S$. 故由紧致性定理可知 $T$ 有模型.

易见 $T$ 的每一模型 $R$ 都具有定理中所说的性质. (证毕)

以下考虑另外一类二次代数整数环 $\mathbf{Z}[\tau] = \{a + b\tau \mid a, b \in \mathbf{Z}\}$, 其中 $\tau = (\sqrt{m} - 1)/2$, $m$ 为任一无平方因子且适合 $m \equiv 1 \pmod 4$ 的有理整数. 我们将证明与定理 5 类似的结论 (见定理 6). 先证明两个引理.

**引理 3** 对于上述的 $m$, 设 $m = 4r + 1$, 则在 $\mathbf{Z}$ 中存在无限多个适合下列性质 $(\Pi_2)$ 的素数 $p$:

$(\Pi_2)$ 对任何 $a, b \in \mathbf{Z}$, 若 $p \nmid a$ 或 $p \nmid b$, 则 $p \nmid a^2 - ab - rb^2$.

**证明** (I) 任取一个不以 $m$ 为平方剩余并且适合 $p \neq 2$, $p \nmid r$ 的素数 (其存在性见下面 (II)). 今证 $p$ 适合 $(\Pi_2)$:

(1.1) 假若有 $a, b \in \mathbf{Z}$ 使: $p \nmid a$ 而 $p | a^2 - ab - rb^2$.

由 $p \nmid a$ 知存在 $l \in \mathbf{Z}$ 使 $al \equiv b \pmod p$. 从而有 $0 \equiv a^2 - ab - rb^2 \equiv a^2(1 - l - rl^2) \pmod p$. 再由 $p \nmid a$ 即有

$$0 \equiv rl^2 + l - 1. \pmod p \tag{1}$$

又由 $p \neq 2$ 知存在 $u \in \mathbf{Z}$ 适合 $2u \equiv 1 \pmod p$, 从而有 $0 \equiv r^2l^2 + rl - r \equiv r^2l^2 + 2url + u^2 - (u^2 + r) \pmod p$. 从而 $4(rl + u)^2 \equiv 4u^2 + 4r \equiv 1 + 4r \equiv m \pmod p$. 所以 $m$ 是模 $p$ 的平方剩余, 这与 $p$ 的取法不合.

所以: 若 $p \nmid a$, 则 $p \nmid a^2 - ab - rb^2$.

(1.2) 假若有 $a, b \in \mathbf{Z}$ 使: $p \nmid b$ 而 $p | a^2 - ab - rb^2$.

由 $p \nmid b$ 知存在 $q \in \mathbf{Z}$ 使 $bq \equiv a \pmod p$. 从而有 $0 \equiv a^2 - ab - rb^2 \equiv b^2(q^2 - q - r) \pmod p$. 再由 $p \nmid b$ 即有 $0 \equiv q^2 - q - r \pmod p$. 由此及 $p \nmid r$ 知 $p \nmid q$, 从而存在 $l_1 \in \mathbf{Z}$ 使 $ql_1 \equiv 1 \pmod p$. 从而 $0 \equiv q^2l_1^2 - ql_1^2 - rl_1^2 \pmod p$, 由此有 $0 \equiv rl_1^2 + l_1 - 1 \pmod p$. 此与 (1.1) 中 (1) 式相同, 再仿 (1.1) 可得矛盾.

所以: 若 $p \nmid b$, 则 $p \nmid a^2 - ab - rb^2$.

由 (1.1) 及 (1.2) 即知 $p$ 适合 $(\Pi_2)$.

(II) 仿引理 1 证明中的 (II), 可知在 $\mathbf{Z}$ 中有无限多个素数 $p$ 不以 $m$ 为平方剩余. 其中适合 $p \neq 2$ 及 $p \nmid r$ 的显然仍有无限多个.

由 (I),(II) 即知引理 3 成立.

**引理 4** 设有理素数 $p$ 适合上述性质 $(\Pi_2)$. 以 $L$ 记 $\mathbf{Z}[\tau]$ 对于理想子环 $(p^3)$ 的剩余类环. 则 $L$ 具有与引理 2 中的 $K$ 相同的性质 (a) 至 (e).

**证明** (a),(b) 易见. 现在证 (c) 至 (e).

(I) 首先, 易见可取下列诸数作为 $L$ 中诸剩余类的代表元:

$$a + b\tau, \quad (0 \leqslant a, b < p^3).$$

所以 $L$ 的元数为 $p^6$.

(II) 现在定出 $L$ 中的单位.

由 $m = 4r + 1$ 及 $\tau = (\sqrt{m} - 1)/2$ 易知有

$$\tau^2 - \tau - r = 0 \tag{1}$$

(2.1) 设 $a + b\tau$ 是 $L$ 的单位，则存在 $L$ 中的元 $x + y\tau$ 适合

$$(a + b\tau)(x + y\tau) = 1, \ (在 L 中) \tag{2}$$

(2) 式左端乘开后用 (1) 可化为 $(ax + rby) + ((a - b)y + bx)\tau$, 所以 (2) 等价于 $\mathbf{Z}$ 中的同余式组

$$ax + rby \equiv 1 \pmod{p^3} \tag{3}$$

$$(a - b)y + bx \equiv 0 \pmod{p^3} \tag{4}$$

由 (3) 可知:

$$p \nmid a \text{ 或 } p \nmid b. \tag{5}$$

(2.2) 反之，若 (5) 成立，则由 ($\text{II}_2$) 知 $p \nmid a^2 - ab - rb^2$. 从而易见存在 $s \in \mathbf{Z}$ 能使

$$(a^2 - ab - rb^2)s \equiv 1 \pmod{p^3} \tag{6}$$

今取 $x, y$ $(0 \leqslant x、y < p^3)$ 使适合 $x \equiv (a - b)s$, $y \equiv -bs \pmod{p^3}$, 则有 (注意 (6))

$$ax + rby \equiv (a^2 - ab)s - rb^2 s \equiv 1 \pmod{p^3},$$

$$(a-b)y + bx \equiv -(a - b)bs + (a - b)bs \equiv 0 \pmod{p^3}.$$

所以 (3),(4) 成立. 从而 $x + y\tau$ 是 $a + b\tau$ 在 $L$ 中的逆元.

(2.3) 由上可知，$a+b\tau$ 在 $L$ 中是单位当且只当 “$p \nmid a$ 或 $p \nmid b$”. 从而易见 $L$ 中单位的个数是 $p^6 - p^4$.

(III) 现在定出 $L$ 中的素元及合元.

(3.1) 先证: $p$ 是 $L$ 中的素元.

任取 $p$ 在 $L$ 中的一个因子分解

$$p=(a+b\tau)(c+d\tau)\ (\text{在 } L \text{ 中}).$$

则在 $\mathbf{Z}$ 中有 (参照 (3) 式的计算):

$$ac+rbd\equiv p\ (\operatorname{mod} p^3) \tag{7}$$

假若 $a+b\tau$ 及 $c+d\tau$ 都不是 $L$ 中的单位, 则由 (2.3) 知应有 $p|a,b,c,d$, 从而有 $p^2|ac+rbd$. 此与 (7) 不合.

所以, $p$ 在 $L$ 中没有真分解, 再由 (2.3) 即知 $p$ 是 $L$ 中的素元.

(3.2) 仿照引理 2 证明中的 (3.2) 至 (3.4), 可以定出 $L$ 的全部素元 ($p^4-p^2$ 个) 及全部合元 ($p^2-1$ 个).

(IV) 仿照引理 2 证明中的 (IV), 可证 $L$ 适合 Goldbacb 性质.

由以上讨论即知 (c),(d),(e) 成立. (证毕)

**定理 6** 对任何形状为 $\mathbf{Z}[\tau]=\{a+b\tau \mid a,b\in\mathbf{Z}\}$ 的二次代数整数环, (其中 $\tau=(\sqrt{m}-1)/2$, $m$ 是无平方因子且适合 $m\equiv 1\ (\operatorname{mod} 4)$ 的有理整数), 都存在具有下列诸性质的扩环 $R$: (a) $R$ 是有 1 的可换环. (b) $R$ 不是整环. (c) $R$ 中有无限多个素元. (d) $R$ 中有无限多个合元. (e) $R$ 适合 Goldbach 性质.

证明仿定理 5, 略去.

## §3 二次数环的不具有 Goldbach 性质的扩环

在本节中, 我们仍以 $\mathbf{Z}[\sqrt{m}]$ 及 $\mathbf{Z}[\tau]$ 分别记定理 5 及定理 6 中所说的两类二次数环.

**引理 5** 设 $p, q$ 是两个不同的适合 $(\Pi_1)$ 的正有理素数，$p > 2$. 以 $K_1$ 记 $\mathbf{Z}[\sqrt{m}]$ 对于理想子环 $(p^2q)$ 的剩余类环. 则 $K_1$ 具有下列诸性质：(a) $K_1$ 是有 1 的可换环. (b) $K_1$ 不是整环. (c) $K_1$ 中存在素元，其个数为 $p^2q^2 - p^2 - q^2 + 1$. (d) $K_1$ 中存在合元，其个数为 $p^4 + q^2 - 2$. (e) $K_1$ 不适合 Goldbach 性质.

证明与下面引理 6 的证法类似，略去.

**定理 7** 对于定理 5 中所说的任何二次代数整数环 $\mathbf{Z}[\sqrt{m}]$ 都存在具有下列诸性质的扩环 $R_1$: (a) $R_1$ 是有 1 的可换环. (b) $R_1$ 不是整环. (c) $R_1$ 中有无限多个素元. (d) $R_1$ 中有无限多个合元. (e) $R_1$ 不适合 Goldbach 性质.

证明与定理 5 者类似，略去.

**引理 6** 设 $p, q$ 是两个不同的适合 $(\Pi_2)$ 的正有理素数，$p > 2$. 以 $L_1$ 记 $\mathbf{Z}[\tau]$ 对于理想子环 $(p^2q)$ 的剩余类环. 则 $L_1$ 具有下列诸性质：(a) $L_1$ 是有 1 的可换环. (b) $L_1$ 不是整环. (c) $L_1$ 中存在素元，其个数为 $p^2q^2 - p^2 - q^2 + 1$. (d) $L_1$ 中存在合元，其个数为 $p^4 + q^2 - 2$. (e) $L_1$ 不适合 Goldbach 性质.

**证明** (a),(b) 易见. 现在证 (c) 至 (e).

(I) 首先，易见可取下列诸数作为 $L_1$ 中诸剩余类的代表元：

$$a + b\tau, (0 \leqslant a, b < p^2q).$$

所以 $L_1$ 的元数为 $p^4q^2$.

(II) 现在定出 $L_1$ 中的单位.

由 $m = 4r + 1$ 及 $\tau = (\sqrt{m} - 1)/2$ 有

$$\tau^2 + \tau - r = 0 \tag{1}$$

(2.1) 设 $a + b\tau$ 是 $L_1$ 的单位，则存在 $L_1$ 中的元 $x + y\tau$ 适合

$$(a + b\tau)(x + y\tau) = 1 \text{ (在 } L_1 \text{ 中)} \tag{2}$$

易知 (2) 等价于 $\mathbf{Z}$ 中的同余式组

$$ax + rby \equiv 1 \pmod{p^2q} \tag{3}$$

$$(a-b)y + bx \equiv 0 \pmod{p^2q} \tag{4}$$

由 (3) 可知：

$$\text{“}p \nmid a \text{ 或 } p \nmid b\text{”}, \tag{5}$$

$$\text{“}q \nmid a \text{ 或 } q \nmid b\text{”}. \tag{6}$$

(2.2) 反之，若 (5) 及 (6) 成立，则由 ($\mathrm{II}_2$) 知 $p, q \nmid a^2 - ab - rb^2$，从而 $p^2q$ 与 $a^2 - ab - rb^2$ 互素，故存在 $s \in \mathbf{Z}$ 能使

$$(a^2 - ab - rb^2)s \equiv 1 \pmod{p^2q} \tag{7}$$

今取 $x, y$ $(0 \leqslant x, y < p^2q)$ 使适合 $x \equiv (a-b)s$, $y \equiv -bs \pmod{p^2q}$，则有 (注意 (7))

$$ax + rby \equiv 1 \pmod{p^2q},$$

$$(a-b)y + bx \equiv 0 \pmod{p^2q}.$$

所以 (3),(4) 成立，从而 $x + y\tau$ 是 $a + b\tau$ 在 $L_1$ 中的逆元.

(2.3) 由上可知，$a + b\tau$ 在 $L_1$ 中为单位当且只当 “(5) 且 (6)”. 故知 $L_1$ 中单位的个数是 $p^2(p^2-1)(q^2-1)$.

(III) 现在定出 $L_1$ 中的素元及合元.

(3.1) 先证：$p$ 是 $L_1$ 中的素元.

任取 $p$ 在 $L_1$ 中的一个因子分解

$$p = (c + d\tau)(f + g\tau) \ (\text{在 } L_1 \text{ 中}).$$

则在 $\mathbf{Z}$ 中有

$$cf + rdg \equiv p \pmod{p^2q},$$

所以存在 $h \in \mathbf{Z}$ 使

$$p = cf + rdg + hp^2q \tag{8}$$

假若 $c+d\tau$ 与 $f+g\tau$ 均非 $L_1$ 的单位，则有

$$(p|c \text{ 且 } p|d) \text{ 或 } (q|c \text{ 且 } q|d),$$
$$(p|f \text{ 且 } p|g) \text{ 或 } (q|f \text{ 且 } q|g).$$

若 $q|c$ 且 $q|d$，则由 (8) 有 $q|p$，此不可能，故必有 $p|c$ 且 $p|d$. 同理有 $p|f$ 且 $p|g$. 由此二结论及 (8) 有 $p^2|p$，又不可能. 所以 $p$ 是 $L_1$ 中的素元.

(3.2) 仿 (3.1) 可证，一切乘积 $p(a+b\tau)$ ($a+b\tau$ 为 $L_1$ 中的单位) 也都是 $L_1$ 中的素元. 其个数可算出 (只需在 $0 \leqslant a,b < pq$ 范围内计算适合 (5) 及 (6) 的 $a+b\tau$ 个数即可) 为 $(p^2-1)(q^2-1)$.

(3.3) 由 (3.1) 可知，一切形如 $p^2(a+b\tau)$ $(0 \leqslant a,b < q)$ 的非 0 元都是 $L_1$ 中的合元. 其个数为 $q^2-1$.

(3.4) 再证： $q$ 是 $L_1$ 中的合元.

由 $p,q$ 互素知存在 $u,v \in \mathbf{Z}$ 能使 $up^2+vq^2=1$，从而易见在 $L_1$ 中有 $q=vq^3$. 由 $q$ 不是单位可知这是 $q$ 的真分解，所以 $q$ 是 $L_1$ 中的合元.

从而一切形如 $q(a+b\tau)$ $(0 \leqslant a,b < p^2)$ 的非 0 元也都是 $L_1$ 中的合元. 其个数为 $p^4-1$.

(3.5) 以上 (2.3),(3.2),(3.3),(3.4) 中已知的单位，素元，合元总数为 $p^4q^2-1$. 所以这已是 $L_1$ 中的全部非 0 元. 由此即得 $L_1$ 中素元及合元的个数.

(IV) 现在证明 $L_1$ 不适合 Goldbach 性质.

考虑 $L_1$ 中的合元 $q$. 由 $L_1$ 中素元的形状易见 $2q$ 不能表示为二素元之和 (注意 $p>2$).　　(证毕)

**定理 8**　对于定理 6 中所说的任何二次代数整数环 $\mathbf{Z}[\tau]$，都存在具有下列诸性质的扩环 $R_1$: (a) $R_1$ 是有 1 的可换环. (b) $R_1$ 不

是整环. (c) $R_1$ 中有无限多个素元. (d) $R_1$ 中有无限多个合元.
(e) $R_1$ 不适合 Goldbach 性质.

证明与定理 5 者类似, 略去.

本节和 § 2 是根据 [8],[9] 改写的. 其它有关讨论可参看 [10], [11] 以及 [12] 等.

## 参考文献


1 Effinger E W, Hayes D R. Additive Number Theory of Polynomials over a Finite Field. New York: The Clarendon Press, 1991

2 Effinger E W, Hayes D R. A complete solution to the polynomial 3–primes problem. Bull. Amer. Math. Soc. (new series), 1991, 24: 363~369

3 王世强. 归纳环及归纳域. 北京师范大学学报, 1988, 24(3): 12~18

4 Wang Sh. Inductive rings and fields. Annals Pure Appl. Logic, 1989, 44: 133~137

5 Chang C C, Keisler H J. Model Theory. Amsterdam: North-Holland Publ. Co., 1973

6 王世强. 某些无限域上多项式环的 Goldbach 3 素元性质. 科学通报, 1998, 43: 821~824

7 Hardy G H, Wright E M. An Introduction to the Theory of Numbers (3rd edition). Oxford: Oxford Univ. Press, 1954

8 王世强. 一类具有 Goldbach 性质的可换环. 北京师范大学学报, 1982, 18(1): 17~22

9 王世强, 武涛. 二次数环的不具有 Goldbach 性质的扩环. 北京师范大学学报, 1982, 18(3): 21~25

10 王世强. 一类不具有 Goldbach 性质的可换环. 数学学报, 1984, 27: 374~380

11 王世强. 一些三次数环的具有及不具有 Goldbach 性质的扩环. 中国科学, 1984(1): 16~23

12 王世强. 一种 Goldbach 可换环的数论性质. 中国科学, 1984(3): 210~216

# 第 5 章

# 关于域上的无限方阵

域上的无限方阵是一类不易处理的对象，现在还缺少一般性的基本研究．它们与有限方阵有很大的不同，例如：无限方阵间一般没有依自然方式定义的乘积，乘积有定义时也未必适合结合律；又如：一个无限方阵可以只有单侧逆方阵而无另一侧的逆方阵，有的无限方阵又会有很多的双侧逆方阵；等等．本章主要讨论行列有限的无限方阵 (简称 rcf 方阵)，它们反映一个域 (看作自身上的向量空间) 的无限直和上的一类线性变换，因而有较好的性质．在 §1 中，讨论 rcf 方阵的求逆问题，我们根据文献 [1] 中关于域上无限线性方程组可解性的一个基本定理 (它可以用模型论方法证明)，得到 rcf 方阵存在各种逆方阵的一些充分必要条件．在 §2 及 §3 中，讨论 rcf 方阵在一种自然的等价性意义下的对角化问题，它比有限方阵的对角化问题要复杂很多．并不是每个 rcf 方阵都可对角化．我们给出 rcf 方阵可对角化的充分必要条件，并给出不可对角化的例子．最后，作为附录，在 §4 中补充说明在 §2 及 §3 中所用到两个概念的存在性．

## § 1 域上 rcf 方阵的逆方阵

在以下的论证中，要多次用到 [1] 中的下列结果：

**定理 1** 设 $F$ 为一域，$E$ 为由 $F$ 上无限个线性方程式所组成的集合 (其中未知量的总个数可为无限多). 如果 $E$ 的每一有限子集都在 $F$ 中有解，则 $E$ 自身在 $F$ 中有解.

这一定理可以用模型论方法证明，大意如下：在一个适当的形式语言上，把域公理及 $F$ 的图象及 $E$ 合起来看作一个形式理论 $T$. 由题设可知 $T$ 的每一有限子集都有模型，故由紧致性定理知 $T$ 自身有模型，任取其一模型 $M$. 由 $T$ 的定义知 $M$ 为 $F$ 的扩域且在其中 $E$ 有解，任取其一组解 $\xi_1, \xi_2, \xi_3, \cdots$. 现在把 $M$ 看作 $F$ 上的向量空间并取定如下一组基底 $b_1 = 1, b_2, b_3, \cdots$(易见此可能). 把诸 $\xi_i$ 依此基底表示为如下形状

$$\xi_i = (x_{i1}, x_{i2}, x_{i3}, \cdots) \ (\text{诸 } x_{ij} \in F),$$

则易见诸 $\xi_i$ 的第 1 分量 $x_{i1}$ $(i = 1, 2, 3, \cdots)$ 就是 $E$ 在 $F$ 中的一组解 (童雪同志也曾独立地得出这一证法).

**定义** 设 $A$ 为域 $F$ 上的无限方阵. 如果 $A$ 的每一行 (列) 中只含有限个非零元，则称 $A$ 为行 (列) 有限的. 如果 $A$ 既是行有限又是列有限的，则称 $A$ 为行列有限的，简称为 rcf- 方阵.

**定义** 设 $A$ 为域 $F$ 上的无限方阵. 如果存在 $A$ 的有限个行 (列) 向量在 $F$ 上线性相关，则称 $A$ 的诸行 (列) 向量在 $F$ 上线性相关. 否则称 $A$ 的诸行 (列) 向量在 $F$ 上线性无关.

**定义** 设 $A$ 为域 $F$ 上列有限的无限方阵. 对于 $A$ 的诸行向量 $r_1, r_2, r_3, \cdots$ 及 $F$ 中任一组元素 $a_1, a_2, a_3, \cdots$，可以依自然方式定义无限线性组合 $a_1r_1 + a_2r_2 + a_3r_3 + \cdots$. 如果存在 $F$ 中一组不全为零的 $a_1, a_2, a_3, \cdots$ 使此线性组合为零向量，则称 $A$ 的诸行向

量在 $F$ 上无限线性相关，否则称 $A$ 的诸行向量在 $F$ 上无限线性无关. 与此对偶，对于 $F$ 上行有限的无限方阵，可以对其诸列向量定义相应的概念.

**定理 2** (a) 设 $A$ 为域 $F$ 上列有限的无限方阵. 则：$A$ 具有 $F$ 上的左逆方阵的充分必要条件是 $A$ 的诸列向量在 $F$ 上线性无关. (b) 与 (a) 对偶的命题.

**证明** 可参照以下定理 3 及定理 4 的证明思路，不在此详述.

对于 $F$ 上的 rcf 方阵 $A$，定理 2 给出了 $A$ 的左逆方阵及右逆方阵存在性的充分必要条件. 但由于这些逆方阵未必也是 rcf 的，从而在它们与 $A$ 之间结合律未必成立，所以我们还不能把定理 2 的 (a),(b) 两部分简单地合起来就直接断言它是 $A$ 具有双侧逆方阵的充分条件，虽然这个结论是对的 (见定理 3). 关于 rcf 方阵的双侧逆方阵的存在性，有下列诸定理.

**定理 3** 设 $A$ 为域 $F$ 上的 rcf 方阵，则 $A$ 具有 $F$ 上的双侧逆方阵的充分必要条件是：$A$ 的诸行向量在 $F$ 上线性无关，并且 $A$ 的诸列向量也在 $F$ 上线性无关.

**证明** (I) 证条件的充分性. 设 $A=(a_{ij})$ 的诸行向量在 $F$ 中线性无关且诸列向量也如此.

由 $A$ 为行列有限可知存在两个正整数函数 $r(i),s(i)$ 能使

$$a_{i,r(i)+1}=a_{i,r(i)+2}=\cdots=0,$$
$$a_{s(i)+1,i}=a_{s(i)+2,i}=\cdots=0.\ (i=1,2,3,\cdots)$$

令 $X=(x_{ij})$ 为由无限个未知量 $x_{ij}$ $(i,j=1,2,3,\cdots)$ 组成的方阵. 现在证明无限方阵的方程组

$$\begin{cases} AX=I, \\ XA=I.\ (I\text{为单位方阵}) \end{cases}$$

在 $F$ 上有解.

首先将此方程组等价地改写为 $F$ 上的一集 (无限多个) 线性方程式如下:

$$E\begin{cases}a_{i1}x_{1j}+a_{i2}x_{2j}+\cdots+a_{ir(i)}x_{r(i)j}=\delta_{ij},\\a_{1j}x_{i1}+a_{2j}x_{i2}+\cdots+a_{s(j)j}x_{is(j)}=\delta_{ij}.\\\quad(i,j=1,2,3,\cdots)\end{cases}$$

(其中 $\delta_{ii}=1$, 当 $i\neq j$ 时 $\delta_{ij}=0$).

任取 $E$ 的有限子集 $E_0$. 设其中出现的最大足码 (不论是行的或列的, $a$ 的或 $x$ 的) 为 $k$. 令 $u=\max(r(1),r(2),\cdots,r(k))$. $v=\max(s(1),s(2),\cdots,s(u))$.

现在考虑 $A$ 左上角的 $v$ 行 $u$ 列子矩阵 $A_1$(易见不妨设 $k\leqslant u\leqslant v$).

由 $v$ 的取法知 $A_1$ 含 $A$ 的前 $u$ 个 "整列"(意指: 在 $A$ 的前 $u$ 个列向量中, 只比 $A_1$ 的相应列向量多出无限个 0 分量). 再由题设可知 $A_1$ 的列秩为 $u$, 从而其行秩也为 $u$.

由 $u$ 的取法仿上段可知, $A_1$ 的前 $k$ 行在 $F$ 上线性无关.

以 $V_1$ 记由 $A_1$ 的行向量生成的向量空间, 则由以上知 $V_1$ 的维数为 $u(\geqslant k)$, 并且以 $A_1$ 的前 $k$ 个行向量为基础可以扩充为 $V_1$ 的一组基底. 设扩充时所需的一组行向量为 $A_1$ 的第 $p_1,p_2,\cdots,p_{u-k}$ 行 (其中 $k<p_1<p_2<\cdots<p_{u-k}\leqslant v$).

为了叙述方便, 现在把 $A$ 的前 $v$ 行重排, 使其: 前 $k$ 行不动; 原第 $p_1,p_2,\cdots,p_{u-k}$ 行各排为第 $k+1,k+2,\cdots,u$ 行; 其他 $v-u$ 个行可任意排序. 记新得的无限方阵为 $A^*$. 则易见 $A^*$ 的左上角 $u\times u$ 方阵 $A_u^*$ 为可逆方阵, 从而有限方阵的方程组

$$\begin{cases}A_u^*Y_u=I_u,\\Y_uA_u^*=I_u.\ (I_u\text{为 } u\times u \text{ 单位方阵})\end{cases}$$

在 $F$ 上有解.

把这一有限方阵方程组等价地改写为 $F$ 上的一组线性方程 $E_n^*$. 我们由 $k$ 的取法不难看出: $E_0$ 实际上可看作 $E_n^*$ 的一部分 (只有所用未知量记号 $x_{ij}$ 与 $y_{ij}$ 的不同). 从而由上段可知 $E_0$ 在 $F$ 中有解. (注意: $E_n^*$ 未必能看作 $E$ 的一部分, 但此事无妨.)

再由 $E_0$ 的任意性及定理 1 即知: $E$ 在 $F$ 中有解. 从而 $A$ 具有 $F$ 上的双侧逆方阵.

(II) 证条件的必要性. 设 $A$ 具有 $F$ 上的双侧逆方阵 $B=(b_{ij})$. 由 $BA=I$ 可知有

$$\begin{cases} 1 = b_{11}a_{11} + b_{12}a_{21} + \cdots + b_{1s(1)}a_{s(1)1}, \\ 0 = b_{11}a_{12} + b_{12}a_{22} + \cdots + b_{1s(2)}a_{s(2)2}, \\ 0 = b_{11}a_{13} + b_{12}a_{23} + \cdots + b_{1s(3)}a_{s(3)3}; \\ \cdots\cdots \end{cases}$$

其中 $s(i)$ 的含义同 (I). 由此易知, $A$ 的第 1 列不能由 $A$ 的另外有限个列在 $F$ 上线性表示.

仿上可知, $A$ 的每一列都不能由 $A$ 的另外有限个列在 $F$ 上线性表示. 从而易见 $A$ 的诸列向量在 $F$ 上线性无关.

同理, 由 $AB=I$ 可知 $A$ 的诸行向量在 $F$ 上线性无关. (证毕)

**引理 1** (a) 设 $A$、$B$ 都是域 $F$ 上行有限的无限方阵, 则对 $F$ 上任何无限方阵 $C$ 都有 $(AB)C=A(BC)$. (b) 设 $A$,$B$ 都是域 $F$ 上列有限的无限方阵, 则对 $F$ 上任何无限方阵 $C$ 都有 $(CB)A=C(BA)$.

**证明** 由直接计算不难看出, 不详述.

**定理 4** (a) 设 $A$ 为域 $F$ 上行有限的无限方阵, 则: $A$ 具有 $F$ 上的行有限左逆方阵的充分必要条件是 $A$ 的诸列向量在 $F$ 上无限线性无关. (b) 与 (a) 对偶的命题.

**证明** (I) 证 (a) 中条件的充分性. 设 $A$ 的诸列向量在 $F$ 上无限线性无关. 以 $r_1, r_2, r_3, \cdots$ 记 $A$ 的诸行向量. 并令 $e_1=(1,0,0,0,\cdots)$, $e_2=(0,1,0,0,\cdots)$, $e_3=(0,0,1,0,\cdots)$, $\cdots$

(1.1) 现在证明：$e_1$ 可由 $r_1, r_2, r_3, \cdots$ 中的有限个在 $F$ 上线性表示.

假若不然，则对每一正整数 $k$, 方程

$$e_1 = x_1 r_1 + x_2 r_2 + \cdots + x_k r_k$$

在 $F$ 中无解. 把此方程等价地改写为 $F$ 上的无限个线性方程

$$E_k \quad \begin{cases} 1 = a_{11}x_1 + a_{21}x_2 + \cdots + a_{k1}x_k, \\ 0 = a_{12}x_1 + a_{22}x_2 + \cdots + a_{k2}x_k, \\ 0 = a_{13}x_1 + a_{23}x_2 + \cdots + a_{k3}x_k, \\ \cdots\cdots \end{cases}$$

(1.1.1) 若 $a_{11}, a_{21}, \cdots, a_{k1}$ 不全为 0.

由 $E_k$ 在 $F$ 中无解及定理 1 易见，存在一正整数 $l = l(k)$ 能使 $E_k$ 的前 $l$ 个方程在 $F$ 中无解. 再由诸方程形状及线性方程组理论易知 $l \geqslant 2$ 并且

$$\begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{k1} \end{bmatrix} \text{可由} \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{k2} \end{bmatrix}, \cdots, \begin{bmatrix} a_{1l} \\ a_{2l} \\ \vdots \\ a_{kl} \end{bmatrix} \text{在 } F \text{ 上线性表示.}$$

(1.1.2) 若 $a_{11}, a_{21}, \cdots, a_{k1}$ 全为 0. 任取 $l \geqslant 2$, 显见仍有与 (1.1.1) 同样的结论成立.

(1.1.3) 以 $c_1, c_2, c_3, \cdots$ 记 $A$ 的诸列向量. 现在考虑方程 $c_1 = x_2 c_2 + x_3 c_3 + \cdots$(由 $A$ 为行有限可知此方程有意义). 把此方程等价地改写为 $F$ 上的一集 (无限多个) 线性方程 $\Delta$, 则由 (1.1.1) 及 (1.1.2)(并注意 $k$ 的任意性) 及定理 1 易知 $\Delta$ 在 $F$ 中有解，从而可知 $c_1, c_2, c_3, \cdots$ 在 $F$ 上无限线性相关. 这与题设矛盾.

(1.2) 仿上可证，每个 $e_i$ 都可由 $r_1, r_2, r_3, \cdots$ 中的有限个在 $F$ 上线性表示 ($i = 1, 2, 3, \cdots$). 由此即易见 $A$ 具有 $F$ 上的行有限左逆方阵.

(II) 证 (a) 中条件的必要性. 设 $A$ 具有 $F$ 上的行有限左逆方阵 $B$. 以 $c_1, c_2, c_3, \cdots$ 记 $A$ 的诸列向量. 若有 $d_1c_1 + d_2c_2 + d_3c_3 + \cdots = 0$(诸 $d_i \in F$), 令 $D = (d_{ij})$, 其中 $d_{i1} = d_{i2} = d_{i3} = \cdots = d_i$ $(i = 1, 2, 3, \cdots)$, 则易见有 $AD = 0$. 再由 $B$ 为行有限及引理 1 可得 $D = (BA)D = B(AD) = 0$, 从而有 $d_1 = d_2 = d_3 = \cdots = 0$. 所以 $c_1, c_2, c_3, \cdots$ 在 $F$ 上无限线性无关.

(b) 的证明与 (a) 完全对偶. (证毕)

**引理 2** (a) 设 $A$ 为域 $F$ 上行有限的无限方阵. 若 $A$ 具有右逆方阵 $C$ 并且具有行有限的左逆方阵 $B$, 则: $B$ 为 $A$ 的唯一双侧逆方阵, 并且是 $A$ 的唯一右逆方阵. (b) 与 (a) 对偶的命题.

**证明** 由引理 1 易见.

由以上诸结果易得下列主要定理:

**定理 5** 设 $A$ 为域 $F$ 上的 rcf 无限方阵, 则: (a) "$A$ 在 $F$ 上具有唯一的双侧逆方阵, 并且它是行有限的" 当且只当: "$A$ 的诸行向量在 $F$ 上线性无关, 并且诸列向量在 $F$ 上无限线性无关". (b) 与 (a) 对偶的命题. (c) "$A$ 在 $F$ 上具有唯一的双侧逆方阵, 并且它也是 rcf 的" 当且只当 "$A$ 的诸行向量在 $F$ 上无限线性无关, 并且诸列向量也在 $F$ 上无限线性无关".

## § 2 域上 rcf 方阵的对角化 (上)

设 $F$ 为任一域. 以下讨论的方阵都是 $F$ 上的.

**定义** 设 $A$ 为一 rcf 方阵. 如果 $A$ 具有 (唯一的)rcf 双侧逆方阵, 则称 $A$ 为 rcf 可逆的.

**定义** 设 $M_1, M_2$ 为 rcf 方阵. 若存在 rcf 可逆的 rcf 方阵 $P, Q$ 能使 $PM_1Q = M_2$, 则称 $M_1$ 与 $M_2$ 等价, 记作 $M_1 \sim M_2$. (易见 $\sim$ 是一等价关系.)

**定义** 设 $D$ 为一 rcf 方阵, 若 $D$ 中的非 0 元都在同一条对角

线上 (不限于主对角线), 则称 $D$ 为一对角方阵. 若 rcf 方阵 $M$ 等价于一个对角方阵, 则称 $M$ 为可对角化的.

关于 rcf 方阵可对角化的充分必要条件, 有以下三个主要定理, 我们先一起列出, 然后再逐步证明.

**定理 6** 对任何自然数 $n$ 及任何 rcf 方阵 $M$, 下列诸条件等价:

$(E_n^1)$ $M \sim D_n = (d_{ij})$, 其中 $d_{11} = d_{22} = \cdots = d_{nn} = 1$, 其他 $d_{ij} = 0$ $(i, j = 1, 2, 3, \cdots)$.

$(L_n^1)$ $M$ 有 $n$ 个行形成一个极大线性无关组.

$(L_n^1)'$ $M$ 有 $n$ 个列形成一个极大线性无关组.

**定理 7** 对任何自然数 $m, n$ 及任何 rcf 方阵 $M$, 下列二条件等价:

$(E_{mn}^2)$ $M \sim D_{mn} = (d_{ij})$, 其中 $d_{m+i,n+i} = 1$, 其他 $d_{ij} = 0$ $(i, j = 1, 2, 3, \cdots)$.

$(L_{mn}^2)$ $M$ 有一个极大线性无关行向量组 $S_r$, $S_r$ 为无限且为无限线性无关, 并且在 $S_r$ 之外 $M$ 还有 $m$ 个行; 同时, $M$ 也有一个极大线性无关列向量组 $S_c$, $S_c$ 为无限且为无限线性无关, 并且在 $S_c$ 之外 $M$ 还有 $n$ 个列.

**定理 8** 对任何 rcf 方阵 $M$, 下列二条件等价:

$(E^3)$ $M \sim D = (d_{ij})$, 其中 $d_{2i-1,2i-1} = 1$, 其他 $d_{ij} = 0$ $(i, j = 1, 2, 3, \cdots)$.

$(L^3)$ $M$ 有一个极大线性无关行向量组 $S_r$, $S_r$ 为无限且为无限线性无关, 并且在 $S_r$ 之外 $M$ 还有无限个行; 同时, $M$ 也有一个极大线性无关列向量组 $S_c$, $S_c$ 为无限且为无限线性无关, 并且在 $S_c$ 之外 $M$ 还有无限个列.

**定理 9** 集合 $\{D_n, D_{mn}, D \mid m, n \in \mathbf{N}\}$ (其中 $\mathbf{N}$ 为自然数集, 诸 $D$ 方阵如定理 6 至 8 所述) 构成互不等价对角方阵的完全系.

**定理 10** rcf 方阵 $M$ 可对角化的充分必要条件是: $M$ 适合

$(L_n^1)$(对某 $n \in \mathbf{N}$) 或 $(L_{mn}^2)$(对某 $m,n \in \mathbf{N}$) 或 $(L^3)$.

定理 6 的证明与有限矩阵时相同, 定理 9 及定理 10 是定理 6 至 8 的推论. 我们现在从一系列引理开始证明定理 7, 到下一节再证明定理 8.

**引理 3** 设 $P, M$ 为 rcf 方阵且 $M$ 的诸行无限线性无关. 令 $M^* = PM$, 并以 $\pi_i, \mu_i$ 及 $\mu_i^*$ $(i = 1,2,3,\cdots)$ 分别记 $P, M$ 及 $M^*$ 的诸行. 如果 $\{\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \cdots\}$ $(i_1 < i_2 < i_3 < \cdots)$ 无限线性无关, 则 $\{\mu_{i_1}^*, \mu_{i_2}^*, \mu_{i_3}^*, \cdots\}$ 也无限线性无关.

**证明** 为使记号简单, 我们只讨论 $i_j = j$ $(j = 1,2,3,\cdots)$ 的情况, 一般情况与此类似.

设 $P = (p_{ij})$, 则由 $M^* = PM$ 有

$$\begin{cases} \mu_1^* = p_{11}\mu_1 + p_{12}\mu_2 + \cdots \\ \mu_2^* = p_{21}\mu_1 + p_{22}\mu_2 + \cdots \\ \cdots\cdots \end{cases}$$

其中诸式右端均为有限和.

设有 $\sum\limits_{i=1}^{\infty} a_i\mu_i^* = 0$, 则由此及上述诸式经整理可得

$$0 = (p_{11}a_1 + p_{21}a_2 + \cdots)\mu_1 + (p_{12}a_1 + p_{22}a_2 + \cdots)\mu_2 + \cdots.$$

再由 $\mu_1, \mu_2, \mu_3, \cdots$ 无限线性无关可得

$$(a_1, a_2, a_3, \cdots)P = (0, 0, 0, \cdots).$$

又由题设及定理 4 的 (b) 知 $P$ 具有列有限的右逆方阵 $Q$, 从而有

$$\begin{aligned} (a_1, a_2, a_3, \cdots) &= (a_1, a_2, a_3, \cdots)(PQ) \\ &= ((a_1, a_2, a_3, \cdots)P)Q = (0, 0, 0, \cdots) \end{aligned}$$

(注意其中的结合律成立). (证毕)

**引理 4** 设 $P, M$ 为行有限的无限方阵且 $P$ 具有行有限的左逆方阵 $Q$, 令 $N = PM$, 并以 $c_i$ 及 $d_i$ $(i = 1, 2, 3, \cdots)$ 分别记 $M$ 及 $N$ 的诸行. 此时, 对域 $F$ 中任何元 $a_1, a_2, a_3, \cdots$ 都有

$$\sum_{i=1}^{\infty} a_i c_i = 0 \text{ 当且只当 } \sum_{i=1}^{\infty} a_i d_i = 0.$$

**证明** 利用等式 $M = QN$ 直接计算即知.

**引理 5** 设 $P, M$ 为 rcf 方阵且 $P$ 为 rcf 可逆. 若 $M$ 适合下列条件

$(L_m^r)$ $M$ 有一个极大线性无关行向量组 $S_r$, $S_r$ 为无限且为无限线性无关, 并且在 $S_r$ 之外 $M$ 还有 $m$ 个行.

则当把 $M$ 换为 $M^* = PM$ 后 $(L_m^r)$ 仍成立.

**证明** (I) 由 $M$ 适合 $(L_m^r)$ 易知存在 rcf 可逆的 rcf 方阵 $R$ 能使

$$M_1 = RM = \begin{pmatrix} O_m \\ M_2 \end{pmatrix},$$

其中 $O_m$ 由 $m$ 个零行组成而 $M_2$ 由 $S_r$ 组成. 从而有 $M^* = P_1 M_1$, 其中 $P_1 = PR^{-1}$ 仍为 rcf 可逆.

(II) 现在把 $P_1$ 表示为 $P_1 = (C_m, P_2)$, 其中 $C_m$ 由 $P_1$ 的前 $m$ 个列组成. 故有 $M^* = P_1 M_1 = P_2 M_2$. 显见 $P_2$ 仍为 rcf, 并且由 $P_1$ 为 rcf 可逆及定理 5 可知 $P_2$ 的诸列无限线性无关.

(III) $P_2$ 的行向量存在极大线性无关组 (参看 § 4), 任取一这样的组 $T_r$. 以下证明: $T_r$ 为无限且为无限线性无关, 并且 $P_2$ 在 $T_r$ 之外还有 $m$ 个行.

(3.1) 假若 $P_2$ 在 $T_r$ 之外有多于 $m$ 个行. 此时易见存在 rcf 可逆的 rcf 方阵 $Q$ 能使 $QP_2$ 的前 $m+1$ 行均为零行. 从而由 $QP_1 = (QC_m, QP_2)$ 可知 $QP_1$ 的前 $m+1$ 行线性相关. 但 $QP_1$ 为 rcf 可逆, 这与定理 5 矛盾. 故此情况不可能出现.

(3.2) 假若 $P_2$ 在 $T_r$ 之外有少于 $m$ 个行. 现在证明此情况也不可能出现. 为使记号简单, 以下用一个有代表性的特例说明此事.

设 $m=3$ 而 $P_2$ 在 $T_r$ 之外有 2 行. 此时 $P_1=(C_3,P_2)$, 并且存在 rcf 可逆的 rcf 方阵 $V$ 能使

$$VP_2=\begin{pmatrix}O_2\\M_3\end{pmatrix},$$

其中 $O_2$ 由 2 个零行组成而 $M_3$ 由 $T_r$ 组成.

现在有

$$VP_1=(VC_3,VP_2),\quad I=((VP_1)^{-1}VC_3,(VP_1)^{-1}VP_2).$$

由后一等式两端各删去前 3 列, 可得

$$\begin{pmatrix}O_3\\I\end{pmatrix}=(VP_1)^{-1}VP_2=(VP_1)^{-1}\begin{pmatrix}O_2\\M_3\end{pmatrix},\tag{1}$$

其中 $O_3$ 由 3 个零行组成.

令 $(VP_1)^{-1}=(a_{ij})$, 由于它 rcf 可逆, 据定理 5 知其前 3 行不能是如下形状

$$\begin{aligned}&(a_{11},a_{12},0,0,0,\cdots)\\&(a_{21},a_{22},0,0,0,\cdots)\\&(a_{31},a_{32},0,0,0,\cdots)\end{aligned}$$

设 (例如) 其第 3 行为

$$(a_{31},a_{32},a_{33},a_{34},0,0,0,\cdots),$$

其中 $a_{33},a_{34}$ 不全为 0. 现在以 $\rho_i(i=1,2,3,\cdots)$ 记 $VP_2$ 的诸行, 并且看 (1) 式两端的第 3 行, 即见有

$$\text{零行}=a_{31}\rho_1+\cdots+a_{34}\rho_4=a_{33}\rho_3+a_{34}\rho_4,$$

所以 $\rho_3,\rho_4$ 线性相关. 但 $\rho_3,\rho_4\in T_r$, 这与 $T_r$ 的取法矛盾.

(3.3) 由以上知 $P_2$ 在 $T_r$ 之外恰有 $m$ 个行. 现在证明 $T_r$ 无限线性无关.

易见存在一 rcf 可逆的 rcf 方阵 $W$ 能使

$$WP_2=\begin{pmatrix}O_m\\M_4\end{pmatrix},$$

其中 $O_m$ 由 $m$ 个零行组成, $M_4$ 由 $T_r$ 组成.

现在考虑 $WP_1=(WC_m,WP_2)$. 以 $\alpha_i,\beta_i$ 及 $\gamma_i$ $(i=1,2,3,\cdots)$ 分别记 $WP_1,WC_m$, 及 $WP_2$ 的诸行. (注意有 $T_r=\{\gamma_{m+1},\gamma_{m+2},\gamma_{m+3},\cdots\}$.)

设有 $F$ 中的元 $b_{m+1},b_{m+2},b_{m+3},\cdots$ 能使 $\sum\limits_{i=m+1}^{\infty}b_i\gamma_i=0$. 现在考虑相应的和 $\sum\limits_{i=m+1}^{\infty}b_i\beta_i=\delta$. 由 $WP_1$ 为 rcf 可逆及定理 5 及 $WP_2$ 的上述形状可知 $\beta_1,\cdots,\beta_m$ 线性无关, 所以 $m$ 维向量 $-\delta$ 可以表示为 $-\delta=\sum\limits_{i=1}^{m}b_i\beta_i$, 从而有 $\sum\limits_{i=1}^{\infty}b_i\beta_i=0$. 此外, 显见又有 $\sum\limits_{i=1}^{\infty}b_i\gamma_i=0$. 由此二等式可得 $\sum\limits_{i=1}^{\infty}b_i\alpha_i=0$, 再由定理 5 即知诸 $b_i$ 均为 0. 所以 $T_r$ 中诸向量为无限线性无关.

(IV) 再以 $\pi_i$ 及 $\mu_i$ $(i=1,2,3,\cdots)$ 分别记 $P_2$ 及 $M^*$ 的诸行. 设 (III) 中的无限线性无关组 $T_r$ 是由 $\pi_{i_1},\pi_{i_2},\pi_{i_3},\cdots$ 组成, 则由 $M^*=P_2M_2$(注意 $M_2$ 的诸行无限线性无关) 及引理 3 知 $M^*$ 的下列行组

$$U_r=\{\mu_{i_1},\mu_{i_2},\mu_{i_3},\cdots\}$$

为无限线性无关 (从而也线性无关).

另外, 由 (III) 中 $T_r$ 的性质可知 $M^*$ 在 $U_r$ 之外恰有 $m$ 个行.

现在, 由 $T_r$ 为 $P_2$ 的极大线性无关行组来证明 $U_r$ 是 $M^*$ 的极大线性无关行组. 任取 $M^*$ 在 $U_r$ 之外的一个行 $\mu_j$, 则相应的 $\pi_j$

可表示为如下形状：

$$\pi_j = c_1\pi_{i_1} + c_2\pi_{i_2} + \cdots + c_h\pi_{i_h},$$

由此及 $M^* = P_2M_2$ 经计算可得

$$\mu_j = c_1\mu_{i_1} + c_2\mu_{i_2} + \cdots + c_h\mu_{i_h}.$$

所以 $U_r$ 是 $M^*$ 的一个极大线性无关行组.

由以上即知 $M^*$ 适合 $(L_m^r)$ (以 $U_r$ 充当其中的 $S_r$). (证毕)

**引理 6** 设 $M = (m_{ij})$ 为一 rcf 方阵, 以 $r_i$ 及 $c_i$ $(i = 1,2,3,\cdots)$ 分别记其诸行及诸列. 若 $\{r_{u+1}, r_{u+2}, r_{u+3},\cdots\}$ 是 $M$ 的一个无限线性无关的极大线性无关行组, 并且 $\{c_{v+1}, c_{v+2}, c_{v+3},\cdots\}$ 是 $M$ 的一个无限线性无关的极大线性无关列组. 令 $N = (n_{ij})$, 其中 $n_{ij} = m_{u+i,v+j}$ $(i,j = 1,2,3,\cdots)$, 则 $N$ 为 rcf 可逆.

**证明** (I) 由题设可知存在 rcf 可逆的 rcf 方阵 $P$ 能使 $PM = M_1$ 的行依次成为

$$0,\cdots,0,r_{u+1},r_{u+2},r_{u+3},\cdots$$

(即：前 $u$ 个行为零行, 其他行与 $M$ 者相同).

以 $d_i$ $(i = 1,2,3,\cdots)$ 记 $M_1$ 的诸列. 由题设及引理 4 可知 $\{d_{v+1}, d_{v+2}, d_{v+3},\cdots\}$ 是 $M_1$ 的一个无限线性无关的极大线性无关列组.

(II) 现在对 $M_1$ 作与 (I) 对偶的论证, 可知存在 rcf 可逆的 rcf 方阵能使 $M_1Q = M_2$ 的列依次成为

$$0,\cdots,0,d_{v+1},d_{v+2},d_{v+3},\cdots.$$

以 $s_i$ $(i = 1,2,3,\cdots)$ 记 $M_2$ 的诸行. 由以上及引理 4 的对偶命题可知 $\{s_{u+1}, s_{u+2}, s_{u+3},\cdots\}$ 是 $M_2$ 的一个无限线性无关的极大线性无关行组.

(III) 现在，由 (I),(II) 及 $N$ 的定义可知

$$M_2 = PMQ = \begin{pmatrix} O_{uv} & O \\ O & N \end{pmatrix},$$

其中 $O_{uv}$ 是 $u \times v$ 零矩阵. 又由 (I) 及 (II) 可知 $N$ 的诸行及诸列均为无限线性无关. 故由定理 5 知 $N$ 为 rcf 可逆. (证毕)

**定理 7 的证明** (I) 由 $(E^2_{mn})$ 证 $(L^2_{mn})$. 由 $(E^2_{mn})$ 知存在 rcf 可逆的 rcf 方阵 $P, Q$ 能使 $M = PD_{mn}Q$.

显见 $D_{mn}$ 适合引理 5 中的 $(L^r_m)$, 故由引理 5 知 $M_1 = PD_{mn}$ 也适合 $(L^r_m)$. 又显见 $D_{mn}$ 适合与 $(L^r_n)$ 对偶的性质 $(L^c_n)$, 故由引理 4 易知 $M_1$ 也适合 $(L^c_n)$.

由于 $M_1$ 适合 $(L^r_m)$ 与 $(L^c_n)$, 再用与以上对偶的论证可知 $M = M_1Q$ 也适合 $(L^r_m)$ 与 $(L^c_n)$, 也即 $M$ 适合 $(L^2_{mn})$.

(II) 由 $(L^2_{mn})$ 证 $(E^2_{mn})$. 以 $r_i$ 及 $c_i$ $(i = 1, 2, 3, \cdots)$ 分别记 $M$ 的诸行及诸列.

(2.1) 若 $\{r_{m+1}, r_{m+2}, r_{m+3}, \cdots\}$ 是 $M$ 的一组无限线性无关的极大线性无关行组, 并且 $\{c_{n+1}, c_{n+2}, c_{n+3}, \cdots\}$ 是 $M$ 的一组无限线性无关的极大线性无关列组. 此时, 仿引理 6 的证法可知存在 rcf 可逆的 rcf 方阵 $P, Q$ 能使

$$PMQ = \begin{pmatrix} O_{mn} & O \\ O & N \end{pmatrix},$$

且其中 $N$ 为 rcf 可逆. 现在令

$$R = \begin{pmatrix} I_m & O \\ O & N^{-1} \end{pmatrix},$$

其中 $I_m$ 为 $m \times m$ 单位方阵, 则易见 $R$ 为 rcf 可逆的 rcf 方阵并且 $RPMQ = D_{mn}$. 所以 $M \sim D_{mn}$.

(2.2) 在一般情况, 由 $(L^2_{mn})$ 易见存在 rcf 可逆的 rcf 方阵 $U, V$ 能使 $UMV$ 成为 (2.1) 的情况, 从而也有 $M \sim D_{mn}$. (证毕)

## § 3　域上 rcf 方阵的对角化 (下)

我们现在继续上节的论证，主要是要证明定理 8，然后给出一个不可对角化 rcf 方阵的例子.

**引理 7**　设 $M$ 为一 rcf 方阵，它有一个无限且余无限的极大线性无关行组 $S_r$，并且 $S_r$ 是无限线性无关的. 令 $N = PM$，其中 $P$ 为一 rcf 可逆的 rcf 方阵，则 $N$ 有一个无限且余无限的极大无限线性无关行组.

**证明**　以 $r_i$ $(i = 1, 2, 3, \cdots)$ 记 $M$ 的诸行. 除了行的重排之外 (这相当于用一个无限的排列方阵左乘)，不妨设 $S_r$ 由 $r_2, r_4, r_6, \cdots$ 组成.

(I) 由所设知可将 $r_1, r_3, r_5, \cdots$ 表示如下：

$$\left.\begin{array}{l} r_1 = a_{12}r_2 + a_{14}r_4 + \cdots \\ r_3 = a_{32}r_2 + a_{34}r_4 + \cdots \\ \cdots\cdots \end{array}\right\} \text{(右端均为有限和)}$$

现在证明，在 $a_{12}, a_{32}, a_{52}, \cdots$ 中只有有限个非零元；同样，在每组 $a_{1,2i}, a_{3,2i}, a_{5,2i}, \cdots$ 中也都如此.

令 $M_2$ 为由 $r_2, r_4, r_6, \cdots$ 组成的方阵 (即 $M_2$ 的第 $i$ 行为 $r_{2i}$). 由定理 4 可知 $M_2$ 有一个列有限的右逆方阵 $K$.

由 $M_2K = I$ 可知 $r_{2i}K = u_i$，其中 $u_i$ 是 $I$ 的第 $i$ 行 $(i = 1, 2, 3, \cdots)$. 由此及以上可得

$$r_1K = a_{12}u_1 + a_{14}u_2 + \cdots = (a_{12}, a_{14}, a_{16}, \cdots)$$

$$r_3K = (a_{32}, a_{34}, a_{36}, \cdots)$$

$$\cdots\cdots$$

这些等式显示出，$a_{12}, a_{32}, a_{52}, \cdots$ 出现在列有限的乘积 $MK$ 第 1 列

中，所以其中只有有限个非零元；类似地，其他每组 $a_{1,2i}, a_{3,2i}, a_{5,2i}, \cdots$ 也都如此.

(II) 现在令 $Q=(q_{ij})$，其中

$$q_{ii}=1,\ q_{2i-1,2j}=-a_{2i-1,2j}, \text{其它}\ q_{ij}=0, (i,j=1,2,3,\cdots).$$

则由 (I) 知 $Q$ 为 rcf 方阵. 又易见 $Q$ 有一 rcf 逆方阵 $R=(r_{ij})$，其中

$$r_{ii}=1,\ r_{2i-1,2j}=a_{2i-1,2j},\ \text{其它}\ r_{ij}=0,\ (i,j=1,2,3,\cdots).$$

令 $M_1=QM$，则 $M_1$ 的诸行为

$$0, r_2, 0, r_4, 0, r_6, \cdots$$

并且 $N=PM=P_1M_1$，其中 $P_1=PR$ 仍为 rcf 可逆.

令 $P_2$ 为由 $P_1$ 的第 $2,4,6,\cdots$ 列 (分别作为 $P_2$ 的第 $1,2,3,\cdots$ 列) 组成的方阵，则有 $N=P_2M_2$. 其中 $M_2$ 的诸行无限线性无关，而 $P_2$ 的诸列无限线性无关.

(III) 现在证明 $P_2$ 具有一个无限且余无限的极大无限线性无关行组.

$P_2$ 具有极大无限线性无关行组 (其证明附述于 § 4). 任取其一，记为 $S_2$.

(3.1) 证 $S_2$ 为无限.

假若 $S_2$ 有限，则由 $P_2$ 为行有限及 $S_2$ 的极大性可知，存在一足码 $j$ 使 $P_2$ 自第 $j$ 列以后均为零列，这与 $P_2$ 诸列的无限线性无关性矛盾.

(3.2) 证 $S_2$ 为余无限.

假若 $S_2$ 为余有限，设 $P_2$ 在 $S_2$ 之外恰有 $n$ 个行. 为使记号简单，以下讨论 $n=5$ 并且 $P_2$ 的前 5 行在 $S_2$ 之外的情况 (一般情况与此类似).

以 $S_i$ $(i=1,2,3,\cdots)$ 记 $P_2$ 的诸行. 由 $S_2$ 的极大性可将 $s_1,\cdots,s_5$ 表示如下:

$$\left.\begin{array}{l} s_1=b_{16}s_6+b_{17}s_7+\cdots \\ \cdots\cdots \\ s_5=b_{56}s_6+b_{57}s_7+\cdots \end{array}\right\} \text{(右端为无限和)}$$

现在令 $U=(u_{ij})$, 其中

$$u_{ii}=1,\ u_{1,5+i}=-b_{1,5+i},\cdots,u_{5,5+i}=-b_{5,5+i},\ \text{其他}\ u_{ij}=0,$$
$$(i,j=1,2,3,\cdots).$$

则 $U$ 为列有限, 且易见有一个列有限的双侧逆方阵 $U^{-1}$.

现在看 $UP_2$. 显见其前 5 行为零行而其他行依次为 $s_6,s_7,s_8,\cdots$. 据此, 并注意到 $P_2$ 为由 $P_1$ 的第 2,4,6,$\cdots$ 列组成, 我们考虑 $UP_1$. 令 $W=P_1^{-1}U^{-1}$, 则有 $I=W(UP_1)$. 比较此式两端偶数足码的列, 可得下列等式

$$\begin{pmatrix} 0\,0\,0\,0\cdots \\ 1\,0\,0\,0\cdots \\ 0\,0\,0\,0\cdots \\ 0\,1\,0\,0\cdots \\ \vdots \\ \vdots \end{pmatrix} = W(UP_2)=W\begin{pmatrix} 0\,0\,0\,0\cdots \\ \cdots\cdots \\ 0\,0\,0\,0\cdots \\ \times\times\times\times\cdots \\ \times\times\times\times\cdots \\ \vdots \end{pmatrix} \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} 5\text{ 个零行} \\ -s_6 \\ -s_7 \\ \vdots \end{array}$$

又由 $I=W(UP_1)$ 易见 $W$ 的诸行线性无关, 所以存在奇数足码 $j$ 能使 $W$ 的第 $j$ 行在第 5 个分量之后还含有非零分量, 设此行为

$$(w_{j1},\cdots,w_{j5},w_{j6},\cdots,w_{jk},0,0,0,\cdots)$$

其中 $k>5$ 且 $w_{j6},\cdots,w_{jk}$ 不全为 0.

现在比较上列方阵等式两端的第 $j$ 行, 可得

$$0=w_{j6}s_6+\cdots+w_{jk}s_k,$$

所以 $s_6,\cdots,s_k$ 线性相关. 这与 $S_2$ 的取法矛盾.

(IV) 由 (III) 及 $N=P_2M_2$ 及引理 3 即见本引理的结论成立.
(证毕)

**引理 8** 设 $M=(m_{ij})$ 为一 rcf 方阵, 以 $r_i$ 及 $c_i$ $(i=1,2,3,\cdots)$ 分别记其诸行及诸列. 设 $r_1,r_3,r_5,\cdots$ 为 $M$ 的一个极大无限线性无关行组, 而 $c_1,c_3.c_5,\cdots$ 为 $M$ 的一个极大无限线性无关列组. 令 $N=(n_{ij})$, 其中

$$n_{ij}=m_{2i-1,2j-1},\ (i,j=1,2,3,\cdots)$$

则 $N$ 为 rcf 可逆.

**证明** (I) 由题设知 $r_2,r_4,r_6,\cdots$ 都可表示为 $r_1,r_3,r_5,\cdots$ 的无限线性组合, 设

$$r_{2i}=\sum_{j=1}^{\infty}a_{2i,2j-1}r_{2j-1},\ (i=1,2,3,\cdots)$$

现在令 $U=(u_{ij})$, 其中

$$u_{ii}=1,\ u_{2i,2j-1}=-a_{2i,2j-1},\ 其他\ u_{ij}=0,\ (i,j=1,2,3,\cdots).$$

$U$ 未必为 rcf 的, 但由其形状易见有如下的双侧逆方阵 $V=(v_{ij})$, 其中

$$v_{ii}=1,\ v_{2i,2j-1}=a_{2i,2j-1},\ 其他\ v_{ij}=0,\ (i,j=1,2,3,\cdots).$$

设 $M_1=UM$, 则 $M_1$ 的诸行为

$$r_1,0,r_3,0,r_5,0,\cdots.$$

又易见 $M=VM_1$. 由此及 $M_1=UM$ 经计算可知, $M$ 的诸列间各种 (有限或无限的) 线性关系与 $M_1$ 的诸列间者完全相同.

以 $s_i$ 及 $d_i$ $(i=1,2,3,\cdots)$ 分别记 $M_1$ 的诸行及诸列，则由题设及以上可知 $s_1,s_3,s_5,\cdots$ 为 $M_1$ 的一个极大无限线性无关行组，而 $d_1,d_3,d_5,\cdots$ 为 $M_1$ 的一个极大无限线性无关列组.

(II) 利用 (I) 中的结论，并进行与 (I) 对偶的论证，可知存在一无限方阵 $W$，它有一个双侧逆方阵，并能使 $M_2=M_1W$ 的诸列成为

$$d_1,0,d_3,0,d_5,0,\cdots.$$

以 $t_i$ 及 $e_i$ $(i=1,2,3,\cdots)$ 分别记 $M_2$ 的诸行及诸列，则 $t_1,t_3,t_5,\cdots$ 为 $M_2$ 的一个极大无限线性无关行组，而 $e_1,e_3,e_5,\cdots$ 为 $M_2$ 的一个极大无限线性无关列组.

(III) 现在比较 $M_2$ 与 $N$ 的形状，即见 $N$ 的诸行及诸列均为无限线性无关，故由定理 5 知 $N$ 为 rcf 可逆.　　(证毕)

**引理 9**　设 $M$ 为一 rcf 方阵，以 $r_i$ 及 $c_i$ $(i=1,2,3,\cdots)$ 分别记其诸行及诸列. 若 $r_1,r_3,r_5,\cdots$ 为 $M_1$ 的一个极大无限线性无关行组，而 $c_1,c_3,c_5,\cdots$ 为 $M_1$ 的一个极大无限线性无关列组，则 $r_1,r_3,r_5,\cdots$ 为 $M_1$ 的一个极大线性无关行组，而 $c_1,c_3,c_5,\cdots$ 为 $M_1$ 的一个极大线性无关列组.

**证明**　沿用引理 8 的记号，可知 $N=(n_{ij})$ 为 rcf 可逆. 设其 (唯一的) 双侧 rcf 逆方阵为 $N^{-1}=(l_{ij})$.

令 $A=(a_{ij})$，其中

$$a_{2i,2i}=1,\ a_{2i-1,2j-1}=l_{ij},\ \text{其它}\ a_{ij}=0,\ (i,j=1,2,3,\cdots).$$

则易见 $A$ 为 rcf 可逆的 rcf 方阵.

(I) 以 $v_i$ 及 $f_i$ $(i=1,2,3,\cdots)$ 分别记 AM 的诸行及诸列. 则

由 $A$ 的形状及 $N^{-1}N = I$ 可得：

$$v_{2i} = r_{2i}, \ (i = 1, 2, 3, \cdots),$$
$$v_1 = (1, x_{12}, 0, x_{14}, 0, x_{16}, 0, \cdots),$$
$$v_3 = (0, x_{32}, 1, x_{34}, 0, x_{36}, 0, \cdots),$$
$$v_5 = (0, x_{52}, 0, x_{54}, 1, x_{56}, 0, \cdots),$$
$$\cdots\cdots.$$

另外，由 $A$ 为 rcf 可逆可知，$AM$ 诸列间的 (有限或无限的) 线性关系与 $M$ 诸列间者全同，从而 $f_1, f_3, f_5, \cdots$ 是 $AM$ 的一个极大无限线性无关列组.

由以上知，$f_2$ 可表示为如下形状：

$$f_2 = \sum_{i=1}^{\infty} k_{2i-1} f_{2i-1}.$$

再由上述诸 $v_i$ 形状经计算可知

$$k_1 = x_{12}, \ k_3 = x_{32}, \ k_5 = x_{52}, \cdots.$$

故由 $AM$ 为列有限知只能有有限个 $k_{2i-1}$ 不为 0, 所以 $f_2$ 只是 $f_1, f_3, f_5, \cdots$ 的有限线性组合.

仿上知 $f_4, f_6, \cdots$ 也都是 $f_1, f_3, f_5, \cdots$ 的有限线性组合. 所以 $f_1, f_3, f_5, \cdots$ 是 $AM$ 的一个极大线性无关列组. 从而 $c_1, c_3, c_5, \cdots$ 是 $M$ 的一个极大线性无关列组.

(II) 仿 (I) 作对偶论证，可知 $r_1, r_3, r_5, \cdots$ 是 $M$ 的一个极大线性无关行组.　　(证毕)

**引理 10**　对任何 rcf 方阵 $M$, 下列二条件等价：

$(L^3)$　$M$ 有一个无限且余无限的极大线性无关行组，它是无限线性无关的；$M$ 也有一个无限且余无限的极大线性无关列组，它是无限线性无关的.

$(L^3)'$ $M$ 有一个无限且余无限的极大无限线性无关行组；$M$ 也有一个无限且余无限的极大无限线性无关列组.

**证明** 由有关定义及引理 9 易见.

**引理 11** (a) 设 $M, P$ 为 rcf 方阵，其中 $P$ 为 rcf 可逆. 若 $M$ 适合定理 8 中的 $(L^3)$, 则 $N = PM$ 也适合 $(L^3)$.

(b) 与 (a) 对偶的命题.

**证明** 只需证 (a) 即可.

(I) 由题设及引理 7 可知 $N$ 有一个无限且余无限的极大无限线性无关行组.

(II) 由题设及引理 4 可知 $N$ 有一个无限且余无限的极大线性无关列组，它是无限线性无关的. 易见它也是 $N$ 的一个极大无限线性无关列组.

(III) 由 (I),(II) 及引理 10 即知 $N$ 适合 $(L^3)$. (证毕)

**定理 8 的证明** (I) 设 $M \sim D$. 此时存在 rcf 可逆的 rcf 方阵 $P, Q$ 能使

$$M = PDQ.$$

显见 $D$ 适合 $(L^3)$, 故由引理 11(a) 知 $PD$ 适合 $(L^3)$, 再由引理 11(b) 即知 $M = (PD)Q$ 适合 $(L^3)$.

(II) 反之，设 $M$ 适合 $(L^3)$. 此时由引理 10 知 $M$ 适合 $(L^3)'$. 令 $S_r$ 为 $M$ 的一个无限且余无限的极大无限线性无关行组，$S_c$ 为 $M$ 的一个无限且余无限的极大无限线性无关列组.

以 $r_i$ 及 $c_i$ $(i = 1, 2, 3, \cdots)$ 分别记 $M$ 的诸行及诸列.

(2.1) 当 $S_r = \{r_1, r_3, r_5, \cdots\}$ 且 $S_c = \{c_1, c_3, c_5, \cdots\}$ 时.

我们沿用引理 8 及引理 9 中的记号，继续论证如下.

易见 $A$ 有一个双侧逆方阵 $B = (b_{ij})$, 其中

$$b_{2i,2i} = 1,\ b_{2i-1,2j-1} = n_{ij},\ 其它\ b_{ij} = 0,\ (i, j = 1, 2, 3, \cdots).$$

由 $M = B(AM)$ 及 $B$ 的形状可知 $r_1, r_3, r_5, \cdots$ 都是 $v_1, v_3, v_5, \cdots$ 的有限线性组合.

又由引理 9 的证明可知 $r_2, r_4, r_6, \cdots$ 都是 $r_1, r_3, r_5, \cdots$ 的有限线性组合.

此外, 我们还有 $v_2 = r_2$, $v_4 = r_4$, $v_6 = r_6, \cdots$. 所以 $v_2, v_4, v_6, \cdots$ 都是 $v_1, v_3, v_5, \cdots$ 的有限线性组合. 设

$$\begin{cases} v_2 = d_{21}v_1 + d_{23}v_3 + \cdots \\ v_4 = d_{41}v_1 + d_{43}v_3 + \cdots \qquad (\text{右端均为有限和}) \\ \cdots\cdots \end{cases}$$

现在令 $E = (e_{ij})$, 其中

$$e_{ii} = 1,\ e_{2i,2j-1} = -d_{2i,2j-1},\ \text{其它}\ e_{ij} = 0,\ (i, j = 1, 2, 3, \cdots).$$

显见 $E$ 是行有限的. 现在说明它也是列有限的.

由 $r_2 = v_2 = d_{21}v_1 + d_{23}v_3 + \cdots$ 及 $v_1, v_3, \cdots$ 的形状可知 $m_{21}$(= $v_2$ 的第 1 分量)= $d_{21}$, 同理有 $m_{41} = d_{41}$, $m_{61} = d_{61}, \cdots$. 故由 $M$ 为列有限及 $E$ 的形状可知 $E$ 的第 1 列只含有限多个非零元. 仿此可知 $E$ 的第 3, 5, 7, $\cdots$ 诸列也都如此. 再由 $E$ 的形状即知 $E$ 是列有限的.

所以 $E$ 是 rcf 方阵, 再由其形状易见 $E$ 有一 rcf 逆方阵.

现在作乘积 $EAM = (h_{ij})$, 则有

$$h_{2i-1,2i-1} = 1,\ h_{2i-1,2j-1} = 0\ (i \neq j),\ h_{2i,j} = 0,\ (i, j = 1, 2, 3, \cdots).$$

最后, 令 $G = (g_{ij})$, 其中

$$g_{ii} = 1,\ g_{2i-1,2j} = -h_{2i-1,2j},\ \text{其它}\ g_{ij} = 0,\ (i, j = 1, 2, 3, \cdots).$$

易见 $G$ 是 rcf 可逆的 rcf 方阵, 并且由计算可知

$$EAMG = D.$$

所以 $M \sim D$.

(2.2) 对于其它情况的 $S_r$ 及 $S_c$, 易见可以把 $M$ 等价地化为一个 $M_0$ 使其相应的 $S_r^0$ 及 $S_c^0$ 适合 (2.1) 的情况，从而有 $M_0 \sim D$. 再由 $M \sim M_0$ 即有 $M \sim D$. (证毕)

由定理 6 至 8 易得定理 9 及定理 10. 由定理 10 可以看出，并不是每个 rcf 方阵都可对角化. 下面举一个不可对角化 rcf 方阵的例子

**例** 令 $M = (m_{ij})$, 其中

$$m_{ii} = 1,\ m_{i+1,i} = -1,\ \text{其它}\ m_{ij} = 0,\ (i, j = 1, 2, 3, \cdots).$$

则 $M$ 不可对角化.

**证明** 假若 $M$ 可对角化，则存在 rcf 可逆的 rcf 方阵 $P = (p_{ij})$, $Q = (q_{ij})$ 及定理 9 中所说的一个对角方阵 $D^*$ 能使 $PMQ = D^*$.

(I) 若 $D^*$ 至少含两个零行. 设其第 $i$ 行及第 $j$ 行为零行 $(i \neq j)$, 则由 $PM = D^*Q^{-1}$ 可得

$$p_{i1} = p_{i2} = p_{i3} = \cdots \text{ 及 } p_{j1} = p_{j2} = p_{j3} = \cdots.$$

所以 $P$ 的第 $i$ 行与第 $j$ 行线性相关. 这与定理 5 矛盾.

(II) 若 $D^*$ 至少含一个零列. 设其第 $i$ 列为零列，则由 $MQ = P^{-1}D^*$ 可得

$$0 = q_{1i} = q_{2i} = q_{3i} = \cdots.$$

所以 $Q$ 含一个零列. 这与定理 5 矛盾.

(III) 若 $D^* = I$. 此时由 $PMQ = I$ 知 $M = P^{-1}Q^{-1}$ 为 rcf 可逆. 但易见 $M$ 的诸行为无限线性相关. 这与定理 5 矛盾.

(IV) 若 $D^* = D_{10}$. 此时由定理 7 知 $M$ 有一个极大线性无关行组 $S_r$, $S_r$ 为无限且为无限线性无关，并且在 $S_r$ 之外 $M$ 还有 1 个行. 但由 $M$ 的形状易见，$M$ 只有一个极大线性无关行组，它包括了 $M$ 的每一行. 所以 $D^*$ 也不可能是 $D_{10}$.

由于情况 (I) 至 (IV) 穷尽了定理 9 中的一切可能性，所以 $M$ 是不可对角化的．　　(证毕)

## §4　rcf 方阵的极大无限线性无关行组

在 §2 及 §3 中，用到了 rcf 方阵 $M$ 的极大线性无关行组 (及列组) 的存在性，也用到了 $M$ 的极大无限线性无关行组 (及列组) 的存在性．作为附录，我们在本节中补充说明这两种极大行组的存在性，并说明其异同．对于列组，有完全对偶的结论成立．

**命题 1**　设 $M \neq 0$ 为一 rcf 方阵，则 $M$ 具有非空的极大线性无关行组．

命题 1 的证明比较简单，只需适当引用 Zorn 引理即可，在此略去．

**命题 2**　设 $M \neq 0$ 为一 rcf 方阵，则 $M$ 具有非空的极大无限线性无关行组．

**证明**　任取 $M$ 的一个非空的极大线性无关行组 $S_0$(由命题 1 知 $S_0$ 存在)．

(I) 若 $S_0$ 为有限组，则易知 $S_0$ 就是 $M$ 的一个极大无限线性无关行组．

(II) 现在考虑 $S_0$ 为无限组的情况．

把 $S_0$ 中的行任意排定一种可数的顺序，记为 $S_0 = \{a_1, a_2, a_3, \cdots\}$．现在按照 $S_0$ 的这种排序，来构作 $S_0$ 的一个子集 $S_\infty$，并证明它是 $M$ 的一个极大无限线性无关行组．(由以下构作法可以看出，对于 $S_0$ 的不同排序，所得到的 $S_\infty$ 可能是不同的．)

(2.1) $S_\infty$ 的构作：

若 $a_1$ 能由 $S_0$ 中其他元无限线性表示，令 $S_1 = S_0 \setminus \{a_1\}$；否则令 $S_1 = S_0$．

若 $a_2$ 能由 $S_1$ 中其他元无限线性表示，令 $S_2 = S_1 \setminus \{a_2\}$；否

则令 $S_2 = S_1$.

……

最后，令 $S_\infty = \bigcap\limits_{i=1}^{\infty} S_i$.

由以上易见，对每个正整数 $i$, 都有：

$$a_i \in S_i \text{ 当且只当 } a_i \in S_\infty. \tag{1}$$

(2.2) 证 $S_\infty$ 不空.

由 $S_0$ 取法知 $a_1 \neq 0$, 设 $a_1$ 的第 $r$ 个分量不为 0. 再由 $M$ 为列有限可知存在正整数 $h$, 能使 $a_h, a_{h+1}, a_{h+2}, \cdots$ 的第 $r$ 个分量均为 0.

假若 $S_\infty$ 为空，则由 $S_\infty$ 的构作法可知：$a_1$ 能由 $\{a_2, a_3, a_4, \cdots\}$ 无限线性表示；$a_2$ 能由 $\{a_3, a_4, a_5, \cdots\}$ 无限线性表示；……. 由此易见 $a_1$ 能由 $\{a_h, a_{h+1}, a_{h+2}, \cdots\}$ 无限线性表示. 再由 $h$ 的取法知 $a_1$ 的第 $r$ 个分量应为 0, 这与 $r$ 的取法矛盾.

(2.3) 证 $S_\infty$ 为无限线性无关.

假若 $S_\infty$ 为无限线性相关，则存在 $a_i \in S_\infty$ 能由 $S_\infty$ $(\subseteq S_{i-1})$ 中其他元无限线性表示，再由 $S_i$ 定义知应 $a_i \notin S_i$, 从而 $a_i \notin S_\infty$. 这与 $a_i$ 的取法矛盾.

(2.4) 证 $S_\infty$ 为 $S_0$ 的极大无限线性无关子集. (从而再由 $S_0$ 取法即易知 $S_\infty$ 为 $M$ 的一个极大无限线性无关行组.)

以下为使记号简单，我们用 $S_\infty$ 的一个特殊情况来说明一般的证明思路. 我们设 $S_\infty = \{a_2, a_4, a_6, \cdots\}$, 并说明 $S_0 \setminus S_\infty$ 中每一元都能由 $S_\infty$ 中的元无限线性表示. 现在以 $a_5$ 为例来说明此事. (对其他 $a_1, a_3, a_7, \cdots$ 也完全类似.)

由 $a_5 \notin S_\infty$ 及 (1) 知 $a_5 \notin S_5$, 故由 $S_5$ 定义知 $a_5$ 能由 $S_4$ 中其他元无限线性表示. 又由 $a_1, a_3 \notin S_\infty$ 及 (1) 易见 $a_1, a_3 \notin S_4$. 所以

$a_5$ 可表示为

$$a_5 = c_2 a_2 + c_4 a_4 + \sum_{i=6}^{\infty} c_i a_i. \qquad (*1)$$

同理，$a_7$ 可表示为 $a_7 = d_2 a_2 + d_4 a_4 + d_6 a_6 + \sum_{i=8}^{\infty} d_i a_i$, 代入 $(*1)$ 并整理后，又可把 $a_5$ 表示为

$$a_5 = c_2' a_2 + c_4' a_4 + c_6' a_6 + \sum_{i=8}^{\infty} c_i' a_i \qquad (*2)$$

同理又可有

$$a_5 = c_2'' a_2 + c_4'' a_4 + c_6'' a_6 + c_8'' a_8 + \sum_{i=10}^{\infty} c_i'' a_i \qquad (*3)$$

$$a_5 = c_2''' a_2 + c_4''' a_4 + c_6''' a_6 + c_8''' a_8 + c_{10}''' a_{10} + \sum_{i=12}^{\infty} c_i''' a_i. \qquad (*4)$$

……

比较 $(*1)$ 及 $(*2)$ 右端. 假若 $c_2 \neq c_2'$, 则易见 $a_2$ 能由 $S_1$ 中的元 $a_4, a_6, a_7, a_8, \cdots$ 无限线性表示，从而应 $a_2 \notin S_2$, $a_2 \notin S_\infty$, 与题设矛盾. 所以 $c_2 = c_2'$, 同理有 $c_2' = c_2'' = c_2''' = \cdots$, 以 $c_2^*$ 记此公共值. 在此基础上，再比较 $(*1), (*2), \cdots$ 的右端，仿上又可知 $c_4 = c_4' = c_4'' = \cdots$, 以 $c_4^*$ 记此公共值. 在此基础上，再比较诸式中 $a_6$ 的系数；然后比较 $(*2)$ 及其以后诸式中 $a_8$ 的系数；然后比较 $(*3)$ 及其以后诸式中 $a_{10}$ 的系数；如此陆续定义 $c_6^*, c_8^*, c_{10}^*, \cdots$.

现在利用这些系数写出下列无限表达式

$$a^* = c_2^* a_2 + c_4^* a_4 + c_6^* a_6 + \cdots \qquad (3)$$

我们来说明 $a_5 = a^*$.

对任一正整数 $l$, 考虑 $a_5$ 的第 $l$ 个分量. 由 $M$ 为列有限可知，存在正整数 $r$, 使 $i > r$ 时诸 $a_i$ 的第 $l$ 个分量均为 0. 又易见，存在

$s \geqslant r$ 能使以上的等式 $(*s)$ 成为

$$a_5 = c_2^* a_2 + c_4^* a_4 + \cdots + c_{2s+2}^* a_{2s+2} + \sum_{i=2s+4}^{\infty} c_i^{(s-1)} a_i.$$

比较此式与 (3) 的右端，并注意 $s$ 的取法，即见两者的第 $l$ 个分量相同.

由上段及 $l$ 的任意性即知 $a_5 = a^*$，所以 $a_5$ 能由 $S_\infty$ 无限线性表示. (证毕)

最后，我们谈谈命题 1 及命题 2 中两种极大无关行组的关系. 对于域上的 rcf 方阵 $M$，这两种极大组有时是一致的 (例如当 $M$ 为 rcf 可逆时)，也有时并不一致. 一般地说， $M$ 的任一极大无限线性无关行组 $S_0$ 显然是一个线性无关行组，从而可以扩大为 $M$ 的一个极大线性无关行组 $S$，但 $S$ 未必等于 $S_0$，如下例所示.

**例** 令 $M = (m_{ij})$ 如下：

$$m_{ii} = 1,\ m_{i+1,i} = -1,\ \text{其他}\ m_{ij} = 0.\ \ (i, j = 1, 2, 3, \cdots)$$

以 $r_i$ $(i = 1, 2, 3, \cdots)$ 记 $M$ 的诸行，则易见 $S = \{r_1, r_2, r_3, \cdots\}$ 是 $M$ 的 (唯一的) 极大线性无关行组. 但 $S$ 是无限线性相关的，因为有

$$r_1 + r_2 + r_3 + \cdots = 0.$$

对任一正整数 $n$，令 $S_n = S \setminus \{r_n\}$，则易知 $S_n$ 为无限线性无关，从而是 $M$ 的一个极大无限线性无关行组.

## 参考文献


1 Abian A. Solvability of infinite systems of linear equations. Archive of Mathematics, 1976, 12: 43~46

2 王世强. 关于域上无限方阵的逆方阵. 北京师范大学学报, 1993, 29: 327~330

3 王世强. On the diagonalization of row–column–finite matrices. 北京师范大学学报, 1997, 33: 321~327

4 Wang Sh. Diagonalization of row–column–finite infinite matrices. Science in China (Series A), 1997, 40: 1279~1286

# 第 6 章

# 共形映射的 1 阶不变量

在复变函数论中，共形映射 (保角映射) 是一个重要的题材. 对于复平面中的两个区域 $G$ 和 $G'$, 如果存在由 $G$ 到 $G'$ 的 1–1 共形映射 (此时称 $G$ 与 $G'$ 为共形等价), 则 $G$ 与 $G'$ 有很多共同的性质 (在以下的论证中可以看到不少例子). 这种共同性质可以看作是 $G$ 在共形等价意义下的不变量. 这方面一个自然而又重要的问题是：对于一个给定的 $G$, 能否找到一组不变量 $I$ 来在共形等价的意义下完全刻划它？ (也就是使得：对任一区域 $G'$, 如果 $G'$ 也具有 $I$ 中的所有性质，则 $G'$ 与 $G$ 共形等价.) 如果存在这样的 $I$, 可以称它为 $G$ 的一组 "共形映射不变量的完全系".

是否对于复平面中每个区域 $G$ 都存在共形映射不变量的完全系？这是一个很困难的问题. 在 1980 年，J. Becker, C. W. Henson 与 L.A. Rubel 在 [1] 中综合运用复变函数论及数理逻辑方法证明了：如果我们对于共形映射不变量作一种较狭义的理解，就是只限于能用 1 阶逻辑的语言来描述的性质 (这需要在一定的形式语言中来理解，详见下), 则 "对于复平面中每一多连通区域都存在共形映射不变量的完全系" 这一命题 (以下简记作 $\mathrm{CSCI}_1$) 是独立于 ZFC 的. 因而它是不可能用通常的朴素集合论来证明或否证的.

本章主要目的就是对 $\mathrm{CSCI}_1$ 的独立性证明大意作一介绍.

## §1 $\mathrm{CSCI}_1$ 与 ZFC 的和谐性

设 $G$ 为复平面中任一区域，以 $H(G)$ 记 $G$ 上全体解析函数对于函数的加法、乘法以及数与函数的乘法所构成的 (复数域 $\mathbf{C}$ 上的) 结合代数.

我们将考虑形式语言 $\mathcal{L}=\{+,\cdot,0,1,\mathrm{i},K\}$ 及 $\mathcal{L}$ 上的 1 阶公式. (其中 $K$ 为 1 元关系符号. 有关概念可参看 [2].) 当取 $H(G)$ 为论域对 $\mathcal{L}$ 上公式作解释时，$\mathcal{L}$ 中的基本符号 $K$ 被解释为"是常函数", 其他基本符号解释如常.

在上述解释下，以 $P(f)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式:

$$[f\text{非单位}]\wedge\forall gh[f=g\cdot h\longrightarrow(g\text{为单位}\vee h\text{ 为单位})].$$

**引理 1** 对任何区域 $G$ 及任何 $f\in H(G)$:

$$[H(G)\models P(f)]\iff[f\text{为 }G\text{ 上的 '点函数'}].$$

($f$ 为 $G$ 上的点函数是指: $f$ 在 $G$ 上有唯一零点，且重数为 1.)

证明易见，略去.

以 $A(f)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式 (其中 $x|y$ 是 $\exists z(x\cdot z=y)$ 的简写):

$$\forall\alpha gh\{[K(\alpha)\wedge P(g)\wedge P(h)\wedge(g|f-\alpha)\wedge(h|f-\alpha)]\longrightarrow(g|h)\}.$$

**引理 2** 对任何区域 $G$ 及任何 $f\in H(G)$:

$$[H(G)\models A(f)]\iff[f\text{在 }G\text{ 上是 1-1 的}].$$

证明易见，略去.

以 $V(\alpha,f,g)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式:

$$[K(\alpha)]\wedge[g\neq 0]\wedge\exists h[P(h)\wedge(h|g)\wedge(h|f-\alpha)].$$

**引理 3** 对任何区域 $G$ 及任何 $\alpha,f,g\in H(G)$:

$$[H(G)\models V(\alpha,f,g)]\iff[(\alpha\text{为常量且 }(g\neq 0)\text{ 且}$$
$$(\text{存在 } z_0\in G\text{ 使 } g(z_0)=0\text{ 而 } f(z_0)=\alpha)].$$

**证明** "必要性" 易见. "充分性". 设 $z_0\in G$ 使 $g(z_0)=0$ 而 $f(z_0)=\alpha$. 今取 $h(z)=z-z_0$, 则 $h\in H(G)$ 且适合 $[P(h)\wedge(h|g)\wedge(h|f-\alpha)]$.

以 $\mathrm{IZ}(g)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式:

$$[g\neq 0]\wedge\exists f[V(0,f,g)\wedge\forall\alpha[V(\alpha,f,g)\to V(\alpha+1,f,g)]].$$

**引理 4** 对任何区域 $G$ 及任何 $g\in H(G)$:

$$[H(G)\models\mathrm{IZ}(g)]\iff[(g\neq 0)\text{且 }(g\text{ 在 }G\text{ 中有无限多个零点})].$$

**证明** (I) "必要性". 易见 $\mathrm{IZ}(g)$ 中所说的 $f$ 在 $g$ 的诸零点处能取到 0,1,2,$\cdots$ 等无限多个值, 从而由 $f$ 的单值性可知 $g$ 在 $G$ 中有无限多个零点. 又由 $\mathrm{IZ}(g)$ 定义知 $g\neq 0$.

(II) "充分性". 由 $g\neq 0$ 及 $g$ 在 $G$ 中有无限多零点可知 $g$ 不是常函数, 从而 $g$ 在 $G$ 中的零点集 $A$ 为 $G$ 的离散子集 (例如参见 [3]p.85 定理 1.2(i)), 从而易知 $A$ 为可数无限集, 可记为 $A=\{\alpha_0,\alpha_1,\alpha_2,\cdots\}$.

由 $A$ 为 $G$ 的离散子集及 $g\in H(G)$ 为连续函数又易知 $A$ 在 $G$ 中无极限点. 故由 [4]p.327 定理 15.13 可知: 存在 $f\in H(G)$ 能使

$$f(\alpha_0)=0,\quad f(\alpha_1)=1,\quad f(\alpha_2)=2,\cdots$$

由此即易见 $H(G)\vDash \mathrm{IZ}(g)$.　　(证毕)

**定理 1**　下列诸集合及关系都能在 $H(G)$ 上用 $\mathcal{L}$ 上的 1 阶公式定义，且定义方式与区域 $G$ 的选择无关：自然数集 $\mathbf{N}$; 整数集 $\mathbf{Z}$; 有理数集 $\mathbf{Q}$; Gauss 有理数集 $\mathbf{Q}(\mathrm{i})$; $\mathbf{N}$ 或 $\mathbf{Z}$ 或 $\mathbf{Q}$ 上的关系 $\leqslant$; $\mathbf{Q}$ 上的绝对值函数.

**证明**　(I) 先考虑 $\mathbf{N}$ 的情况. 以 $N(\alpha)$ 记 $\mathcal{L}$ 上 (任一个) 表达下列含义的 1 阶公式:

$$\forall fg\{[V(0,f,g)\wedge\forall\beta(V(\beta,f,g)\to V(\beta+1,f,g))]\to V(\alpha,f,g)\}.$$

(1.1) 若 $\alpha$ 为一自然数, 易见有 $H(G)\vDash N(\alpha)$ 成立.

(1.2) 反之, 若有 $H(G)\vDash N(\alpha)$ 成立, 任取 $G$ 的一个可数无限且在 $G$ 中无极限点的子集 $A$(此种 $A$ 的存在性易见). 由 [4] p.326 定理 15.11 可知存在一 $g\in H(G)$ 能使其零点集恰为 $A$. 再仿上述引理 4 的证法可找到一个 $f\in H(G)$ 使 $f$ 在 $A$ 上的值集恰为自然数集 $\mathbf{N}$. 易见此二 $f,g$ 适合 $N(\alpha)$ 中的 "$[\cdots]$" 再由 $N(\alpha)$ 成立即知 $V(\alpha,f,g)$ 成立, 故由 $f$ 的取法知 $\alpha$ 为一自然数.

(1.3) 综合 (1.1) 及 (1.2) 即知: 对任何区域 $G$ 及任何 $\alpha\in H(G)$ 都有

$$[\alpha\in\mathbf{N}]\iff[H(G)\vDash N(\alpha)].$$

(II) 在 (I) 的基础上, 即易于定义其他所述集合及关系如下:

$$[\alpha\in\mathbf{Z}]\iff[\alpha\in\mathbf{N}\vee(-\alpha)\in\mathbf{N}].$$

$$[\alpha\in\mathbf{Q}]\iff\exists\beta\gamma[\beta\in\mathbf{Z}\wedge\gamma\in\mathbf{Z}\wedge\gamma\neq0\wedge\alpha\gamma=\beta].$$

$$[\alpha\in\mathbf{Q}(\mathrm{i})]\iff\exists\beta\gamma[\beta\in\mathbf{Q}\wedge\gamma\in\mathbf{Q}\wedge\alpha=\beta+\gamma\mathrm{i}].$$

在 $\mathbf{Q}$ 上: $[\alpha\leqslant\beta]\iff\exists\gamma\delta[\gamma\in\mathbf{N}\wedge\delta\in\mathbf{N}\wedge\gamma\neq0\wedge\gamma(\beta-\alpha)=\delta]$.
(在 $\mathbf{N}$ 或 $\mathbf{Z}$ 上, $\alpha\leqslant\beta$ 的定义更显然, 略去.)

在 $\mathbf{Q}$ 上: $[|\alpha| = \beta] \iff [0 \leqslant \beta \wedge (\beta = \alpha \vee \beta = -\alpha)]$. (证毕)

**引理 5** 以 $\Delta(f,g,\sigma)$ 记 $\mathcal{L}$ 上 (任一个) 表达下列含义的 1 阶公式:

$$\forall\alpha \in \mathbf{C}\exists hk\exists\beta \in \mathbf{C}\exists\gamma \in \mathbf{C}[(\sigma - \alpha\text{为单位}) \vee (g = \beta + (\sigma - \alpha)h \\ \wedge f = \gamma + \beta(\sigma - \alpha) + k(\sigma - \alpha)^2].$$

(其中: $\forall\alpha \in C\{\cdots\}$ 表示 $\forall\alpha\{K(\alpha) \to \cdots\}$; $\exists\beta \in C\{\cdots\}$ 表示 $\exists\beta\{K(\beta) \wedge \cdots\}$; ($\sigma - \alpha$ 为单位) 表示 $\exists\delta\{(\sigma - \alpha)\delta = 1\}$.) 则对任何区域 $G$ 及任何 $f, g, \sigma \in H(G)$ 之 $\sigma$ 为 1–1 者, 都有

$$[H(G) \vDash \Delta(f,g,\sigma)] \iff [\text{在 } \sigma(G) \text{ 上有 } (g \circ \sigma^{-1})(f \circ \sigma^{-1})'].$$

**证明** (I) "必要性". 对任一 $z \in G$, 令

$$\alpha = \sigma(z), \tag{1}$$

则 $\sigma - \alpha$ 在 $G$ 上非单位, 故由 $\Delta(f,g,\sigma)$ 成立知 $g = \beta + (\sigma - \alpha)h$ 且 $f = \gamma + \beta(\sigma - \alpha) + k(\sigma - \alpha)^2$.

对任何 $w \in \sigma(G)$, 由 $f = \gamma + \beta(\sigma - \alpha) + k(\sigma - \alpha)^2$ 可得

$$\begin{aligned}(f \circ \sigma^{-1})(w) &= \gamma + \beta(\sigma(\sigma^{-1}(w)) - \alpha) + k(\sigma^{-1}(w))(\sigma(\sigma^{-1}(w)) - \alpha)^2 \\ &= \gamma + \beta(w - \alpha) + k(\sigma^{-1}(w))(w - \alpha)^2,\end{aligned}$$

对 $w$ 微分, 得

$$(f \circ \sigma^{-1})'(w) = \beta + (w - \alpha)[\cdots],$$

今取 $w = \alpha$ (注意由 (1) 知 $\alpha \in \sigma(G)$), 得

$$(f \circ \sigma^{-1})'(\alpha) = \beta. \tag{2}$$

又由 $g=\beta+(\sigma-\alpha)h$ 可得

$$(g\circ\sigma^{-1})(w)=\beta+h(\sigma^{-1}(w))(\sigma(\sigma^{-1}(w))-\alpha)$$
$$=\beta+h(\sigma^{-1}(w))(w-\alpha)$$

再取 $w=\alpha$, 得

$$(g\circ\sigma^{-1})(\alpha)=\beta. \tag{3}$$

由 (1) 知 $\alpha$ 为 $\sigma(G)$ 中任一点，故由 (2) 及 (3) 知在 $\sigma(G)$ 上有 $(g\circ\sigma^{-1})=(f\circ\sigma^{-1})'$.

(II) "充分性". 设在 $\sigma(G)$ 上有 $(g\circ\sigma^{-1})=(f\circ\sigma^{-1})'$. (注意由 $\sigma$ 为 $G$ 上的 1–1 解析函数可知 $\sigma^{-1}$ 为由 $\sigma(G)$ 到 $G$ 上的 1–1 解析函数.)

任取复数 $\alpha$. 若 $\sigma-\alpha$ 为 $H(G)$ 中的单位，则由 $\Delta$ 定义知其中的 $[\cdots]$ 已成立. 若 $\sigma-\alpha$ 非 $H(G)$ 中的单位，则易见 $\alpha\in\sigma(G)$, 在 $\alpha$ 处把 $g\circ\sigma^{-1}$ 及 $f\circ\sigma^{-1}$ 展开，则由 $(g\circ\sigma^{-1})=(f\circ\sigma^{-1})'$ 知二展式为如下形状

$$(g\circ\sigma^{-1})(w)=\beta+(w-\alpha)h_1(w),$$
$$(f\circ\sigma^{-1})(w)=\gamma+\beta(w-\alpha)+(w-\alpha)^2k_1(w)$$

$(w\in\sigma(G))$. 对任何 $z\in G$, 令 $w=\sigma(z)$, 代入上二式得:

$$g(z)=\beta+(\sigma(z)-\alpha)h_1(\sigma(z)),$$
$$f(z)=\gamma+\beta(\sigma(z)-\alpha)+(\sigma(z)-\alpha)^2k_1(\sigma(z)),$$

记 $h_1\circ\sigma$ 为 $h$, $k_1\circ\sigma$ 为 $k$, 即得 $g=\beta+(\sigma-\alpha)h$ 及 $f=\gamma+\beta(\sigma-\alpha)+k(\sigma-\alpha)^2$.

综上所述，即知 $\Delta(f,g,\sigma)$ 在 $H(G)$ 中成立. (证毕)

**定理 2** 存在 $\mathcal{L}$ 上的 1 阶公式 $E(x,y)$ 能使: 对任何区域 $G$ 及任何 $\alpha,\beta\in H(G)$,

$$[H(G)\vDash E(\alpha,\beta)] \iff [\alpha,\beta \text{ 为复数且 } \mathrm{e}^{\alpha}=\beta].$$

**证明** 以 $E(x,y)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式:

$$\exists\sigma f[(\sigma\text{为 1-1})\wedge(x\text{ 及 0 都在 }\sigma\text{ 的值域中})$$
$$\wedge\,(f(0)\underset{\sigma}{=}1)\wedge(f(x)\underset{\sigma}{=}y)\wedge((f\circ\sigma^{-1})=(f\circ\sigma^{-1})')]$$

($f(x)\underset{\sigma}{=}y$ 的含义见下).

(I) 先说明上述含义确能在 $\mathcal{L}$ 上 1 阶地表达.

(1.1) 由引理 2 知 ($\sigma$ 为 1–1) 可用 $A(\sigma)$ 表达.

(1.2) ($x$ 在 $\sigma$ 的值域中) 等价于 ($K(x)\wedge(\sigma-x)$ 非单位).

(1.3) ($f(x)\underset{\sigma}{=}y$) 表示

$$[K(x)\wedge K(y)\wedge A(\sigma)\wedge(\sigma-x\text{ 非单位})\wedge((\sigma-x)|(f-y))],$$

其含义为: "对于此 $x,y$ 及 1–1 的 $\sigma$ 而言, 当 $\sigma$ 取 $x$ 值时, $f$ 取 $y$ 值."

(1.4) $(f\circ\sigma^{-1})=(f\circ\sigma^{-1})'$ 可用引理 5 中的 $\Delta(f,f,\sigma)$ 表达.

(II) 证 "必要性". 习知, 指数函数 $g=\mathrm{e}^z$ 在 0 的任一邻域内可由 $g(0)=1$ 及函数方程 $g=g'$ 唯一决定. 所以当 $H(G)\vDash E(\alpha,\beta)$ 成立时, 由 $E(x,y)$ 的含义可知 $f\circ\sigma^{-1}$ 在 $\sigma(G)$ 上为指数函数 $\mathrm{e}^z$, 再由 ($f(\alpha)\underset{\sigma}{=}\beta$) 即知 $\mathrm{e}^\alpha=\beta$.

(III) 证 "充分性". 设对复数 $\alpha,\beta$ 有 $\mathrm{e}^\alpha=\beta$ 成立. 任取 $G$ 上一个 1–1 的解析函数 $\sigma$ 之值域包含 0 及 $\alpha$ 者 (易见 $\sigma$ 存在), 再令 $f(z)=\mathrm{e}^{\sigma(z)}$(对一切 $z\in G$), 则 $\sigma,f\in H(G)$ 且能使 $E(\alpha,\beta)$ 中的 $[\cdots]$ 成立, 从而有 $H(G)\vDash E(\alpha,\beta)$. (证毕)

**引理 6** 设 $m\geqslant 2$ 为一正整数, 则存在 $\mathcal{L}$ 上的 1 阶公式 $E_m(x,y)$ 能使: 对任何区域 $G$ 及任何 $\alpha,\beta\in H(G)$,

$$[H(G)\vDash E_m(\alpha,\beta)]\iff[\alpha,\beta\text{ 为复数且 }m^\alpha=\beta].$$

证明的思路与定理 2 者类似 (注意 $m^\alpha=\mathrm{e}^{\alpha\ln m}$ 并利用上述的 $E(x,y)$), 略去.

**引理 7** 存在 $\mathcal{L}$ 上的 1 阶公式 $R(x)$ 能使：对任何区域 $G$ 及任何 $\alpha \in H(G)$,

$$[H(G) \models R(\alpha)] \iff [\alpha\text{为一实数}].$$

证明较长，略去．可参看 [1]pp141~145．(注意：本章的 $H(G)$ 即该文的 $H_C(G)$, 本章的 $\mathcal{L}$ 即该文中的 "algebra language".)

利用 $R(x)$, 即可在 $\mathcal{L}$ 上定义实数间的 $\leqslant$ 及复数的绝对值如下：

在实数集 $\mathbf{R}$ 上： $[\alpha \leqslant \beta] \iff \exists\gamma[R(\gamma) \wedge \beta = \alpha + \gamma^2]$.

在复数集 $\mathbf{C}$ 上： $[|\alpha| = \beta] \iff \exists\gamma\delta[R(\gamma) \wedge R(\delta) \wedge \alpha = \gamma + \delta\mathrm{i} \wedge \exists\lambda(R(\lambda) \wedge \beta = \lambda^2) \wedge \beta^2 = \gamma^2 + \delta^2]$.

**定理 3** 如果 "存在 $\mathcal{P}(\mathbf{N})$(自然数集 $\mathbf{N}$ 的幂集) 的一个良序，它是在自然数系 $(\mathbf{N}, +, \cdot)$ 上可以 2 阶定义的", 则复平面中每一区域 $G$ 都是对语言 $\mathcal{L}$ 范畴的．("$G$ 对 $\mathcal{L}$ 是范畴的" 是指："对复平面中任一区域 $G'$, 如果 $H(G')$ 与 $H(G)$ 适合 $\mathcal{L}$ 上完全相同的 1 阶语句，则存在由 $G'$ 到 $G$ 上的 1-1 共形映射".)

**证明** (I) 先证明：在定理题设下，可以写出 $\mathcal{L}$ 上一个 1 阶公式 $L(f_1, f_2, g_1, g_2, k)$ 使此 $L$ 在幂集 $\mathcal{P}(\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+)$ 上定义一个良序 $\leqslant$(其中 $\mathbf{Q}^+$ 为正有理数集).

(1.1) 设 $W(X, Y)$ 是自然数系 $(\mathbf{N}, +, \cdot)$ 的语言 $\{+, \cdot, 0, 1\}$ 上一个 2 阶公式，它能使在 $\mathcal{P}(\mathbf{N})$ 上如下定义的关系 $\leqslant$ 是 $\mathcal{P}(\mathbf{N})$ 上的一个良序：

$$[A \leqslant B] \text{ 当且只当 } [(\mathbf{N}, +, \cdot) \models W(A, H)]$$

(对一切 $A, B \in \mathcal{P}(\mathbf{N})$)．由定理题设知 $W(X, Y)$ 存在.

由于自然数的 $n$ 元组能用一种确定的可定义方式编码为一自然数，从而 $\mathbf{N}$ 上的每一 $n$ 元关系都可通过此种编码转化为 $\mathbf{N}$ 的

一个子集. 所以我们不妨设 $W(X,Y)$ 中不含有 2 阶的关系量词, 只含有 2 阶的集合量词及 1 阶的数目量词.

以下, 我们要根据 $W(X,Y)$ 作出 $\mathcal{L}$ 上一个 1 阶公式 $L(f_1,f_2,g_1,g_2,k)$, 使此 $L$ 能在幂集 $\mathcal{P}(\mathbf{Q}(\mathrm{i})\times\mathbf{Q}^+)$ 上定义一个良序 $\leqslant$.

(1.2) 对 $W(X,Y)$ 作如下的改造, 可得 $\mathcal{L}$ 上一个 1 阶公式 $W^*(f,g,k)$:

(i) 把每一数目量词 $\exists x\{\cdots\}$ 改为 $\exists x\{N(x)\wedge\cdots\}$, 其中 $N(x)$ 的定义见定理 1. 类似地, 把每一 $\forall x\{\cdots\}$ 改为 $\forall x\{N(x)\to\cdots\}$. (必要时改变 $N(x)$ 中的约束变元, 以下仿此.)

($\mathrm{ii}_1$) 取定三个互异的函数变元 $f,g,k$. 把 $X,Y$ 各换为 $f,g$.

($\mathrm{ii}_2$) 对于在 $W(X,Y)$ 中出现的 $X,Y$ 之外的 (约束的) 集合变元 $Z_1,\cdots,Z_r$, 取定 $r$ 个函数变元 $h_1,\cdots,h_r$ 并作如下处理:

把每一集合量词 $\exists Z_i\{\cdots\}$ 改为

$$\exists h_i\{\forall\alpha[V(\alpha,h_i,k)\to N(\alpha)]\wedge\cdots\},$$

把每一集合量词 $\forall Z_i\{\cdots\}$ 改为

$$\forall h_i\{\forall\alpha[V(\alpha,h_i,k)\to N(\alpha)]\to\cdots\},$$

其中 $V(x,y,z)$ 的定义见引理 3 处.

(iii) 把每一形如 $(t\in Z_i)$ 的原子公式改为 $V(t,h_i,k)$; 把每一形如 $(t\in X)$ 或 $(t\in Y)$ 的原子公式分别改为 $V(t,f,k)$ 或 $V(t,g,k)$.

(iv) 把如上所得的公式记为 $U(f,g,k)$, 令 $W^*(f,g,k)$ 为 $\mathrm{IZ}(k)\wedge U(f,g,k)\wedge\forall\alpha[(V(\alpha,f,k)\vee V(\alpha,g,k))\to N(\alpha)]$, 其中 $\mathrm{IZ}(x)$ 的定义见引理 4 处.

(1.3) 设 $G$ 为任一区域, $k\neq 0$ 为 $H(G)$ 中任一个在 $G$ 中具有无限多零点的函数, 则易知: 对任何 $f,g\in H(G)$ 都有

$$[H(G)\vDash W^*(f,g,k)]\ 当且只当$$

$$[A_f\subseteq\mathbf{N}且\ A_g\subseteq\mathbf{N}\ 且\ A_f\leqslant A_g],$$

其中 $A_f = \{\alpha |\ \exists z \in G(f(z) = \alpha \wedge k(z) = 0)\}$, $A_g$ 仿此.

(1.4) 利用 $\mathcal{P}(\mathbf{N})$ 上的良序 $\leqslant$, 可以依如下方式导出 $\mathcal{P}(\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+)$ 上的一个良序，仍记为 $\leqslant$:

$\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+$ 中每一序偶 $(q,r)$ 可以唯一地表示为

$$q = (-1)^a \frac{b}{c} + (-1)^d \frac{e}{f}\mathrm{i}, \quad r = \frac{a'}{b'},$$

其中： $a$ 为 0 或 1; $d$ 为 0 或 1; $b,c,e,f,a',b' \in \mathbf{N}$; $c,f,a',b' \neq 0$; $b,c$ 互素； $e,f$ 互素； $a',b'$ 互素. 据此，由序偶 $(q,r)$ 可唯一地映射到一个自然数

$$2^a 3^b 5^c 7^d 11^e 13^f 17^{a'} 19^{b'}.$$

(显见不同的序偶映射到不同的自然数，并且只有一部分自然数能如此被映射到.)

依照上述映射，可以由 $\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+$ 的每一子集得到 $\mathbf{N}$ 的一个子集, 从而就能依自然方式由 $\mathcal{P}(\mathbf{N})$ 上的良序 $\leqslant$ 得到 $\mathcal{P}(\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+)$ 上的一个良序 $\leqslant$.

(1.5) 令 $L(f_1, f_2, g_1, g_2, k)$ 为 $\mathcal{L}$ 上任一个表达下列含义的公式 (为便于阅读，在一些对应括号处加了相同的下标):

$$\begin{aligned}
&\mathrm{IZ}(k) \wedge \exists \varphi\psi\{_0 \forall \alpha\beta\gamma\{_1[_2 K(\alpha) \wedge K(\beta) \wedge K(\gamma) \wedge (k|f_1 - \alpha)\\
&\wedge (k|f_2 - \beta) \wedge (k|\varphi - \gamma)]_2 \leftrightarrow \exists abcdefa'b'[_3 N(b) \wedge N(c) \wedge N(e) \wedge\\
&N(f) \wedge N(a') \wedge N(b') \wedge c \neq 0 \wedge f \neq 0 \wedge a' \neq 0 \wedge b' \neq 0\\
&\wedge \forall xyz[_4[_5 N(x) \wedge N(y) \wedge N(z) \wedge ((xy = b \wedge xz = c) \vee (xy =\\
&e \wedge xz = f) \vee (xy = a' \wedge xz = b'))]_5 \rightarrow x = 1]_4 \wedge [_6(a =\\
&0 \wedge d = 0 \wedge cf\alpha = bf + ce\mathrm{i}) \vee (a = 0 \wedge d = 1 \wedge cf\alpha = bf - ce\mathrm{i})\\
&\vee (a = 1 \wedge d = 0 \wedge cf\alpha = -bf + ce\mathrm{i}) \vee (a = 1 \wedge d = 1 \wedge cf\alpha =\\
&-bf - ce\mathrm{i})]_6 \wedge \exists \gamma_1\gamma_2 \cdots \gamma_8[_7 E_2(a, \gamma_1) \wedge E_3(b, \gamma_2) \wedge E_5(c, \gamma_3) \wedge\\
&E_7(d, \gamma_4) \wedge E_{11}(e, \gamma_5) \wedge E_{13}(f, \gamma_6) \wedge E_{17}(a', \gamma_7) \wedge E_{19}(b', \gamma_8) \wedge
\end{aligned}$$

$\gamma = \gamma_1\gamma_2\cdots\gamma_8]_7]_3\}_1 \wedge\forall\alpha\beta\gamma\{_8[_9 K(\alpha)\wedge K(\beta)\wedge K(\gamma)\wedge(k|g_1 - \alpha) \wedge (k|g_2 - \beta) \wedge (k|\psi - \gamma)]_9 \leftrightarrow \exists abcdefa'b'[_{10}\cdots]_{10}\}_8\wedge W^*(\varphi,\psi,k)\}_0$

(其中 $E_m(x,y)$ 定义见引理 6 处; $[_{10}\cdots]_{10}$ 与 $[_3\cdots]_3$ 全同). 并令 $A(f_1,f_2) = \{(\alpha,\beta)|\exists z \in G(f_1(z) = \alpha \wedge f_2(z) = \beta \wedge k(z) = 0)\}$. $A(g_1,g_2)$ 仿此.

设 $G$ 为任一区域, $k \neq 0$ 为 $H(G)$ 中任一个在 $G$ 中具有无限多零点的函数, 则不难证明: 对任何 $f_1,f_2,g_1,g_2 \in H(G)$ 都有

$$[H(G) \vDash L(f_1,f_2,g_1,g_2,k)] \text{ 当且只当}$$
$$[A(f_1,f_2) \subseteq \mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+ \text{ 且 } A(g_1,g_2) \subseteq \mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+$$
$$\text{且 } A(f_1,f_2) \leqslant A(g_1,g_2)].$$

(II) 以 $V(\alpha,\beta,f_1,f_2,k)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式: (在 $H(G)$ 中)"存在一个点函数 $p$ 使 $(p|k)$ 且 $(p|f_1-\alpha)$ 且 $(p|f_2-\beta)$" (参看引理 1).

再以 $F(\sigma)$ 记 $\mathcal{L}$ 上任一个表达下列含义的 1 阶公式:

$(\sigma$ 为 $1\text{–}1)\wedge\forall\tau\{(\tau$ 为 $1\text{–}1)\longrightarrow [_1\forall k f_1 f_2 g_1 g_2[_2[_3\mathrm{IZ}(k) \wedge\forall\alpha\beta[_4 V(\alpha,\beta,f_1,f_2,k) \leftrightarrow (\alpha \in \mathbf{Q}(\mathrm{i}) \wedge \beta \in \mathbf{Q}^+ \wedge \{\gamma \in \mathbf{C}\big||\alpha-\gamma| < \beta\} \subseteq \mathrm{range}(\sigma))]_4 \wedge \forall\alpha\beta[_5 V(\alpha,\beta,g_1,g_2,k) \leftrightarrow (\alpha \in \mathbf{Q}(\mathrm{i}) \wedge \beta \in \mathbf{Q}^+ \wedge\{\gamma \in \mathbf{C}\big||\alpha-\gamma| < \beta\} \subseteq \mathrm{range}(\tau))]_5]_3 \rightarrow L(f_1,f_2,g_1,g_2,k)]_2]_1\}$.

其中 $\mathbf{C}$ 为复数集. (注意: $x \in \mathrm{range}(y)$ 可表示为 $K(x)\wedge(y-x$非单位).)

(III) 对任一区域 $G$, 令

$$\mathcal{R}(G) = \big\{(q,r) \in \mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+\big|\{\alpha \in \mathbf{C}\big||q-\alpha| < r\} \subseteq G\big\}.$$

则由上述 $F(\sigma)$ 的含义可以看出，对任何区域 $G$ 及任何 $\sigma \in H(G)$ 都有：

$[H(G) \models F(\sigma)]$ 当且只当 $[\sigma$ 是 $G$ 上的 1-1 共形映射；

并且在由 $L$ 所定义的 $\mathcal{P}(\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+)$ 的良序 $\leqslant$ 下，对 $G$ 上的任何 1-1 共形映射 $\tau$，都有 $\mathcal{R}(\sigma(G)) \leqslant \mathcal{R}(\tau(G))]$.

(IV) 现在证明：复平面中每一区域 $G$ 都是对语言 $\mathcal{L}$ 为范畴的.

(4.1) 设 $G$ 为任一区域. 令 $G_0$ 为 "与 $G$ 共形等价并且在 $\mathcal{P}(\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+)$ 的良序 $\leqslant$ 下 $\mathcal{R}(G_0)$ 为最小" 的那个区域 (易见 $G_0$ 由 $\mathcal{R}(G_0)$ 唯一决定).

设 $G'$ 为任一能使 "$H(G')$ 与 $H(G)$ 适合 $\mathcal{L}$ 上完全相同的 1 阶语句" 的区域. 以下证明： $G'$ 与 $G$ 为共形等价. 有此之后，即知 $G$ 对 $\mathcal{L}$ 是范畴的.

(4.2) 令 $G_0'$ 为 "与 $G'$ 共形等价并且在 $\mathcal{P}(\mathbf{Q}(\mathrm{i}) \times \mathbf{Q}^+)$ 的良序 $\leqslant$ 下 $\mathcal{R}(G_0')$ 为最小" 的那个 (唯一的) 区域. 现在证明 $\mathcal{R}(G_0) = \mathcal{R}(G_0')$. 由对称性，我们只需证明 $\mathcal{R}(G_0) \subseteq \mathcal{R}(G_0')$.

设 $(q,r) \in \mathcal{R}(G_0)$, 则 $\mathcal{L}$ 中 (任一个) 表达下列含义的语句

$$\forall\sigma\big[F(\sigma) \longrightarrow \big\{\alpha \in \mathbf{C}\big|\,|q-\alpha| < r\big\} \subseteq \mathrm{range}(\sigma)\big]$$

在 $H(G)$ 中成立. (这是因为：由 $G_0$ 定义及 $F(\sigma)$ 含义可知，当 $F(\sigma)$ 成立时， $\mathrm{range}(\sigma)$ 必为 $G_0$, 再参照 $\mathcal{R}(G_0)$ 定义即知上式成立.) 再由 $G'$ 取法可知此语句也在 $H(G')$ 中成立，从而再由 $G_0'$ 定义及 $F(\sigma)$ 含义及 $\mathcal{R}(G_0')$ 定义又有 $(q,r) \in \mathcal{R}(G_0')$. 所以 $R(G_0) \subseteq R(G_0')$.

(4.3) 由 $\mathcal{R}(G)$ 定义易见有

$$G = \bigcup_{(q,r)\in\mathcal{R}(G)} \big\{\alpha \in \mathbf{C}\big|\,|q-\alpha| < r\big\},$$

所以由上段的 $\mathcal{R}(G) = \mathcal{R}(G_0)$ 可得 $G_0 = G_0'$. 再由 $G_0$ 及 $G_0'$ 定义

即知 $G$ 与 $G'$ 为共形等价.　　（定理 3 证毕）

**定理 4**　(I) 存在 ZFC 的模型 $M_1$, 在其中连续统假设成立, 并且在其中存在 $\mathcal{P}(\mathbf{N})$ 的一个良序, 它可以用关于自然数系 $(\mathbf{N},+,\cdot)$ 的 2 阶公式来定义.　(II) 存在 ZFC 的模型 $M_2$, 在其中连续统假设不成立, 并且在其中存在 $\mathcal{P}(\mathbf{N})$ 的一个良序, 它可以用关于自然数系 $(\mathbf{N},+,\cdot)$ 的 2 阶公式来定义.

(I) 的证明可参看 [5] p527.

(II) 的证明可参看 [6].

由定理 3 及定理 4 即可得下列的

**主定理 1**　(I) 存在 ZFC 的模型 $M_1$, 在其中连续统假设成立, 并且在 $M_1$ 中：复平面中每一区域 $G$ 都是对语言 $\mathcal{L}$ 范畴的.　(II) 存在 ZFC 的模型 $M_2$, 在其中连续统假设不成立, 并且在 $M_2$ 中：复平面中每一区域 $G$ 都是对语言 $\mathcal{L}$ 范畴的.

## § 2　"非 $\mathrm{CSCI}_1$" 与 ZFC 的和谐性

**定义**　设 $F(x,y_1,\cdots,y_n)$ 为集合论语言 $\{\in\}$ 中的一个公式. 如果由 ZFC 能推出如下语句：

$$\forall GG'y_1\cdots y_n\{[(G\text{与 }G'\text{ 都是复平面 }\mathbf{C}\text{ 中的区域})\\ \wedge(G\text{与 }G'\text{ 为共形等价})]\to[F(G,y_1,\cdots,y_n)\leftrightarrow F(G',y_1,\cdots,y_n)]\},$$

则称公式 $F(x,y_1,\cdots,y_n)$ 为 **共形不变的**.

**例**　熟习公理集合论的读者不难看出, 可以在语言 $\{\in\}$ 中写出一个 1 阶公式 $F(x,y)$, 它在通常的语义解释下表达如下的含义："$x$ 是复平面 $\mathbf{C}$ 中的一个区域而 $y$ 是 $\mathcal{L}$ 中一个语句, 并且 $y$ 在 $H(x)$ 中成立." ($F(x,y)$ 的具体写出是很冗长的, 在此略去. 不熟习公理集合论的读者可以暂时承认 $F(x,y)$ 的存在.) 容易看出, $F(x,y)$ 是一个共形不变的公式.

任意取定 ZFC 的一个模型 $(M,\in)$ 使其 $M$ 为可数可迁集者，(由公理集合论可知，这样的模型可以适合连续统假设，也可以不适合.) 再任取整数集 $\mathbf{Z}$ 的一个子集 $S$ 使其为 "generic over $M$" 者. 以 $M[S]$ 记由 $M\cup\{S\}$ 生成的 ZFC 的可迁模型. (由公理集合论可知，当且只当 $M$ 适合连续统假设时，$M[S]$ 适合连续统假设.) 则用力迫法可证下列定理.

**定理 5** 设 $M,S$ 如上述. 定义 $\mathbf{Z}$ 的子集 $S_0$, $S_1$ 如下：

$$S_0=\{n\in\mathbf{Z}\mid 2n\in S\},\quad S_1=\{n\in\mathbf{Z}\mid 2n+1\in S\}.$$

则有：

(I) 在 ZFC 的模型 $(M[S],\in)$ 中，其复平面上不存在形如 $T(z)=az+b$ 的映射能把 $S_0$ 映到 $S_1$ 上.

(II) 若 $F(x,y_1,\cdots,y_n)$ 是语言 $\{\in\}$ 中一个 1 阶公式，并且对每一 $m\in\mathbf{Z}$ 都能在 ZFC 中推出下列公式：

$$\forall u\subseteq\mathbf{Z}[F(u,y_1,\cdots,y_n)\leftrightarrow F(u+m,y_1,\cdots,y_n)]$$

(其中 $u+m$ 代表把 $u$ 中每个元素 $v$(为整数) 都换 $v+m$ 所得的集合)，则在模型 $(M[S],\in)$ 中，对任何 $a_1,\cdots,a_n\in M$ 都有下式成立：

$$F(S_0,a_1,\cdots,a_n)\leftrightarrow F(S_1,a_1,\cdots,a_n).$$

证明略去.

**定理 6** 设 $M,S,S_0,S_1$ 如定理 5 所述. 在 ZFC 的模型 $(M[S],\in)$ 中，令 $G_0=\mathbf{C}\setminus S_0$, $G_1=\mathbf{C}\setminus S_1$ ($\mathbf{C}$ 为复平面). 则：

(I) $G_0$ 与 $G_1$ 在 $(M[S],\in)$ 中不为共形等阶.

(II) 对任何共形不变公式 $F(x,y_1,\cdots,y_n)$ 及任何 $a_1,\cdots,a_n\in M$, 在 $(M[S],\in)$ 中有下式成立：

$$F(G_0,a_1,\cdots,a_n)\leftrightarrow F(G_1,a_1,\cdots,a_n).$$

**证明** (I) 在集合论模型 $(M[S],\in)$ 中引用复变函数论来证明 $G_0$ 与 $G_1$ 不为共形等价:

假若在 $(M[S],\in)$ 中存在一个由 $G_0$ 到 $G_1$ 上的 1-1 共形映射 $T$, 则用 Picard 大定理易证 (注意由 $S$ 取法知其为无限集): 存在 $a,b\in\mathbf{C}$ 使 $T(z)=az+b$ (对一切 $z\in G_0$). 此 $T$ 可自然地看作定义在全部 $\mathbf{C}$ 上的映射, 并易见其必把 $S_0$ 映到 $S_1$ 上. 这与定理 5 的 (I) 矛盾.

(II) 设 $F(x,y_1,\cdots,y_n)$ 为一共形不变公式. 据此定义一新公式 $H(z,y_1,\cdots,y_n)$, 使表达下列含义:

$$z\subseteq\mathbf{Z}\wedge F(\mathbf{C}\setminus z,y_1,\cdots,y_n),$$

则易见对每一 $m\in\mathbf{Z}$, 都可在 ZFC 中推出下式:

$$\forall z\subseteq\mathbf{Z}[H(z,y_1,\cdots,y_n)\leftrightarrow H(z+m,y_1,\cdots,y_n)].$$

从而由定理 5 的 (2) 可知, 对任何 $a_1,\cdots,a_n\in M$, 在 $(M[S],\in)$ 中都有下式成立:

$$H(S_0,a_1,\cdots,a_n)\leftrightarrow H(S_1,a_1,\cdots,a_n).$$

由此及 $H$ 的上述含义即知在 $(M[S],\in)$ 中也有

$$F(G_0,a_1,\cdots,a_n)\leftrightarrow F(G_1,a_1,\cdots,a_n).$$

成立. (证毕)

**主定理 2** (I) 存在 ZFC 的模型 $M_3$, 在其中连续统假设成立, 并且在 $M_3$ 中: 存在整数集 $\mathbf{Z}$ 的子集 $S_3$, 使复平面 $\mathbf{C}$ 中的区域 $\mathbf{C}\setminus S_3$ 对语言 $\mathcal{L}$ 不是范畴的.

(II) 存在 ZFC 的模型 $M_4$, 在其中连续统假设不成立, 并且在 $M_4$ 中: 存在整数集 $\mathbf{Z}$ 的子集 $S_4$, 使复平面 $\mathbf{C}$ 中的区域 $\mathbf{C}\setminus S_4$ 对语言 $\mathcal{L}$ 不是范畴的.

**证明**　视定理 6 中的 $(M[S],\in)$ 为 $M_3$(当 $M$ 适合连续统假设时) 或 $M_4$(当 $M$ 不适合连续统假设时). 令 $S_0=\{n\in\mathbf{Z}|2n\in S\}$, 并令 $G_0$ 为 (在 $(M[S],\in)$ 中的) 区域 $\mathbf{C}\setminus S_0$. 以下证明, 在模型 $(M[S],\in)$ 中, $G_0$ 对 $\mathcal{L}$ 不是范畴的 (从而 $S_0$ 即可充当主定理中的 $S_3$ 及 $S_4$).

依定理 6 定义区域 $G_1$, 则由定理 6 知 $G_0$ 与 $G_1$ 在 $(M[S],\in)$ 中不为共形等价.

假若 $G_0$ 在 $(M[S],\in)$ 中对 $\mathcal{L}$ 是范畴的, 则由上段可知存在 $\mathcal{L}$ 上的 1 阶语句 $A$, 它在 $H(G_0)$ 中为真而在 $H(G_1)$ 中为假.

但是, $A$ 实际上可看作 $M$ 中的一个集合 (不熟习公理集合论的读者可暂时承认此事). 所以对前述例子中的共形不变公式 $F(x,y)$(见定理 5 之前), 据定理 6 之 (II) 可知, 在 $(M[S],\in)$ 中有

$$F(G_0,A)\leftrightarrow F(G_1,A)$$

成立. 再由此 $F(x,y)$ 所表达的含义 (见上例), 就可看出 (注意 $G_0,G_1$ 都是 $\mathbf{C}$ 中的区域) $A$ 在 $H(G_0)$ 及 $H(G_1)$ 中的真假情况应该相同. 这与上段矛盾.

所以, 在 $(M[S],\in)$ 中, $G_0$ 对 $\mathcal{L}$ 不是范畴的.　　　(证毕)

由主定理 1 及主定理 2, 就可得到本章开始处所说的独立性结论. 从而看出, 在复变函数论的研究中, 有些自然提出的重要问题, 其解决也是离不开数理逻辑方法的. 这种问题, 在多元复变函数论中也是存在的, 读者可参看文献 [7], 此处不再多谈.

## 参考文献

1 Becker J, Henson C W, Rubel L A. First-order conformal invariants. Annals of Math. (new series), 1980, 112: 123~178

2 王世强. 模型论基础. 北京: 科学出版社, 1987

3 Lang S. Complex Analysis. London: Addison–Wesley Publ. Co., 1977

4 Rudin W. Real and Complex Analysis. New York: McGraw–Hill, 1974

5 Jech Th. Set Theory. New York: Academic Press, 1978

6 Harrington L. Long projective well orderings. Annals of Math. Logic, 1977, 12: 1～24

7 Lempert L, Rubel L A. An independence result in several complex variables. Proc. Amer. Math. Soc., 1991, 113: 1055～1065

# 第 7 章

# 代数封闭群与模型论

代数封闭群是人们熟知的代数封闭域概念在群论中的类似物. 其定义为:

设 $G$ 为一群, 如果由系数在 $G$ 中的任何有限个群论方程式所构成的方程组 $\Sigma$ 都在 $G$ 中有解, 则称 $G$ 为一 **代数封闭群**.

换言之, 在这样的群 $G$ 中, 对于 "解 (有限) 方程组" 的代数要求总是可行的, 不需要对 $G$ 进行扩张, 所以名曰 "代数封闭".

如果把上述的代数要求加强, 使有限组 $\Sigma$ 中不限于只含等式, 而是也允许含有不等式, 就得到一类性质更强的群, 称为存在封闭群. 但这时的 $\Sigma$ 不能是任意写出的, 因为它可能是无解的矛盾组 (例如 $\Sigma_1 = \{x \neq x\}$, $\Sigma_2 = \{ax = y, a^{-1}y \neq x\}$, 等等), 所以需要对 $\Sigma$ 加上 "无矛盾" 的要求. 对于 "无矛盾" 性, 一个合理的提法是 "$\Sigma$ 可以在 $G$ 的某一扩群中有解". 因而存在封闭群的定义是:

设 $G$ 为一群, 如果对于由系数在 $G$ 中的任何有限个群论方程及不等式所构成的联立组 $\Sigma$, 当 $\Sigma$ 在 $G$ 的某个扩群中有解时, $\Sigma$ 在 $G$ 中也有解, 则称 $G$ 为一 **存在封闭群**.

代数封闭群和存在封闭群都是代数性质很好的群. (后者是前者的真子类. 例如易知单位元群 $G = \{1\}$ 是代数封闭群而不是

存在封闭群.）这些群虽然自身有趣，但关于它们的纯代数研究却往往不易深入，而需借助一些数理逻辑方法，包括模型论及递归论方法.

代数封闭群的概念是 W. R. Scott 于 1951 年提出的 (见 [1])，后来有 G. Higman, B. H. Neumann, H. Neumann 及 A. Macintyre, M. Ziegler, W. Hodges 等人分别用代数方法及逻辑方法进行了越来越深入的研究. 读者可参看 G. Higman 与 E. Scott 的专著 [2] 及 W. Hodges 的模型论专著 [3] 及其中所引文献.

本章取材于 [3], 对其中有关存在封闭群的主要结果 (主要是关于各种可数代数封闭群的存在性, 见以下定理 A,B,C,D) 及其论证方法作了精简及改写，目的在于用不太长的篇幅向广大数学工作者介绍数理逻辑方法在这方面的应用简况. 本章不要求读者具备群论或数理逻辑方面专门的预备知识，只要有一定的数学修养即可阅读. （以下用到少数模型论概念及符号，可参看 [4]).

## §1 群论 $\exists_1$ 公式的结式

**定义** 设 $T$ 为语言 $\mathcal{L}$ 上的 1 阶理论 (即：由 $\mathcal{L}$ 上一些 1 阶语句所构成的集合. 以下简称理论), $\overline{x}=(x_1,\cdots,x_n)$ 为一组取定的互异变元， $\varphi(\overline{x})$ 为 $\mathcal{L}$ 上一个 $\exists_1$ 公式 (即： $\varphi(\overline{x})$ 为前束标准形，并且其前束词中没有全称量词), 以 $\mathrm{Res}_\varphi(\overline{x})$ 记 $\mathcal{L}$ 上全体适合

$$T\vdash\forall\overline{x}(\varphi(\overline{x})\to\psi(\overline{x}))$$

的 $\forall_1$ 公式 $\psi(\overline{x})$ (即： $\psi(\overline{x})$ 为前束标准形，并且其前束词中没有存在量词) 所构成的集合. 称 $\mathrm{Res}_\varphi(\overline{x})$ 为 $\varphi(\overline{x})$ 的结式.

**定理 1** 设 $T$ 为语言 $\mathcal{L}$ 上的理论， $A$ 为 $\mathcal{L}$ 的模型， $\overline{a}$ 为 $A$ 中的 $n$ 元组， $\varphi(\overline{x})$ 为 $\mathcal{L}$ 上的 $\exists_1$ 公式 (其中 $\overline{x}=(x_1,\cdots,x_n)$). 则下列二条件等价：

(a) 存在 $T$ 的模型 $B \supseteq A$ 适合 $B \models \varphi(\overline{a})$.

(b) $A \models \wedge\mathrm{Res}_\varphi(\overline{a})$. ($\wedge\mathrm{Res}_\varphi(\overline{x})$ 表示 $\mathrm{Res}_\varphi(\overline{x})$ 中一切公式的合取. 它是一个非 1 阶的无限长语句, 以自然方式作语义解释.)

**证明** (1) 由 (a) 证 (b):

由 $B \models \varphi(\overline{a})$ 及 $B \models T$ 及 $\mathrm{Res}_\varphi(\overline{x})$ 定义易知有 $B \models \wedge\mathrm{Res}_\varphi(\overline{a})$. 再由 $B \supseteq A$ 及 $\mathrm{Res}_\varphi(\overline{x})$ 中均为 $\forall_1$ 公式即易见有 (b) 成立.

(2) 由 (b) 证 (a):

设 $A \models \wedge\mathrm{Res}_\varphi(\overline{x})$. 令 $\mathcal{L}_1 = \mathcal{L} \cup \{d_1, \cdots, d_n\}$, 其中 $d_1, \cdots, d_n$ 为互异的新常量. 在 $A$ 中用 $a_i$ 解释 $d_i(i = 1, \cdots, n)$, 则 $A$ 膨胀为 $\mathcal{L}_1$ 的模型 $D$.

设 $\exists_1$ 公式 $\varphi(\overline{x})$ 为 $\exists\overline{y}\psi(\overline{x}, \overline{y})$, 其中 $\overline{y} = (y_1, \cdots, y_m)$ 而 $\psi(\overline{x}, \overline{y})$ 无量词.

令 $\mathcal{L}' = (\mathcal{L}_1)_D \cup \{c_1, \cdots, c_m\}$, ($c_1, \cdots, c_m$ 为互异的新常量.) 考虑 $\mathcal{L}'$ 上的理论

$$T' = T \cup \mathrm{diag}(D) \cup \{\psi(\overline{d}, \overline{c})\},$$

其中 $\mathrm{diag}(D)$ 为 $D$ 的图象. 以下证 $T'$ 和谐.

假若 $T'$ 不和谐, 则由紧致性定理知存在 $T'$ 的有限子集不和谐, 从而易见存在 diag$(D)$ 中有限个语句的合取 $\theta(\overline{d}, \overline{b})$ 能使

$$T \cup \{\psi(\overline{d}, \overline{c})\} \vdash \neg\theta(\overline{d}, \overline{b}),$$

其中 $\overline{b}$ 为 $(\mathcal{L}_1)_D \setminus \mathcal{L}$ 中 $\overline{d}$ 之外的一组常量. 由上式及谓词演算可得

$$T \cup \{\psi(\overline{d}, \overline{c})\} \vdash \forall\overline{z}\neg\theta(\overline{d}, \overline{z}),$$

由此又可得

$$T \vdash \exists\overline{y}\psi(\overline{d}, \overline{y}) \to \forall\overline{z}\neg\theta(\overline{d}, \overline{z}),$$

$$T \vdash \forall\overline{x}(\varphi(\overline{x}) \to \forall\overline{z}\neg\theta(\overline{x}, \overline{z})).$$

从而可知 $\forall\overline{z}\neg\theta(\overline{x},\overline{z})\in \mathrm{Res}_{\varphi}(\overline{x})$, 再由题设 (b) 有

$$A\models\forall\overline{z}\neg\theta(\overline{a},\overline{z}).$$

由上式易见有 $D\models\forall\overline{z}\neg\theta(\overline{d},\overline{z})$, 从而有 $D\models\neg\theta(\overline{d},\overline{b})$. 但由 $\theta(\overline{d},\overline{b})$ 的取法又有 $D\models\theta(\overline{d},\overline{b})$, 故得矛盾. 所以 $T'$ 和谐.

任取 $T'$ 的模型 $B'$, 将其归约到语言 $\mathcal{L}$ 上, 记为 $B$. 则由 $T'$ 的构成易见有 $B\supseteq A$, 并且 $B\models\varphi(\overline{a})$. (证毕)

设 $G$ 为一群, $a,b\in G$. 以下把 $b^{-1}ab$ 简记为 $a^b$, 把 $a^{-1}b^{-1}ab$ 简记为 [a,b].

**定理 2**(Higman) 设 $G$ 为一有限生成的群. 则 $G$ 能递归地给出的充分必要条件是: $G$ 能嵌入一个有限给出的群中.

证明可参看专著 [5] 第 IV.7 节.

**定理 3** 设 $G$ 为一群, $H$ 与 $K$ 均为 $G$ 的子群且存在一同构映射 $\alpha: H\to K$. 则存在群 $G'\supseteq G$ 及其中一元 $g$ 能使: 对一切 $h\in H$ 都有 $g^{-1}hg=\alpha(h)$.

证明可参看 [5] 第 IV.2 节.

**定理 4** 设 $G$ 为一群, $g_i(i=0,1,2,\cdots)$ 为 $G$ 中任一系列元素 (不论同异). 则存在群 $G'\supseteq G$ 及其中二元 $a,b$ 能使 $g_i=[[a,b^{2i+1}],a]$, $(i=0,1,2,\cdots)$.

证明可参看 [6].

在讨论群时, 我们取语言 $\mathcal{L}=\{\cdot,{}^{-1},1\}$, 并令 $T$ 为群的 1 阶理论如下:

$$\begin{aligned}T=\{&\forall xyz((xy)z=x(yz)),\ \forall x(xx^{-1}=1\wedge x^{-1}x=1),\\&\forall x(x1=x\wedge 1x=x)\}\end{aligned}$$

(注意 $T$ 为 $\forall_1$ 理论).

**引理 1** 在群的理论 $T$ 之下, 对每一正整数 $n$, 公式

$$(x_1=1\wedge\cdots\wedge x_n=1)\to(y=1)$$

等价于 (对理论 $T$) 下列 $\exists_1$ 公式的结式:

$$\exists u_1 v_1 w_1 \cdots u_n v_n w_n (y = \prod_{1 \leqslant i \leqslant n} (x_i^{u_i} x_i^{v_i} x_i^{w_i})).$$

证明 (1) 当 $n = 1$ 时.

(1.1) 一方面, 对任一群 $G$ 中的任何元 $a, b$, 若有 $\exists uvw(b = a^u a^v a^w)$ 成立, 显见有 $(a = 1 \to b = 1)$ 成立.

(1.2) 另一方面, 对任一群 $G$ 中任何元 $a, b$, 设有 $(a = 1 \to b = 1)$ 成立. 以下再分二情况.

(1.2.1) 若 $b = 1$. 在 $G$ 之外取两个与 $\langle a \rangle_G$ (指 $a$ 在 $G$ 中生成的子群) 同构且互异的循环群 $C, D$, 并设 $c, d$ 各为 $C, D$ 的一个生成元. 考虑群 $G \times C \times D$, 在其中 $a, c, d, cd$ 的周期相同, 故由定理 3(连用 3 次) 可知, 存在一群 $H \supseteq G \times C \times D$ 及其中的元 $u, v, w$ 能使 $a^u = c$, $a^v = d$, $(cd)^w = a^{-1}$. 从而易见在 $H$ 中有 $(1 =) b = a^1 a^{uw} a^{vw}$.

(1.2.2) 若 $b \neq 1$, 则也有 $a \neq 1$. 此时, 在 $G$ 之外取一个与 $\langle a \rangle_G$ 同构的循环群 $C$ 及其一生成元 $c$. 考虑自由积 $G * C$. 由自由积性质可知 $ca$ 与 $c^{-1}b$ 都周期无限. 故由定理 3 知存在群 $H \supseteq G * C$ 及其中的元 $u, v$ 能使 $a^u = c$ 及 $(ca)^v = c^{-1}b$. 从而在 $H$ 中有 $b = a^u a^{uv} a^v$.

由以上及定理 1 即易见 $n = 1$ 时引理成立.

(2) 当 $n > 1$ 时.

(2.1) 一方面, 对任一群 $G$ 中的任何元 $a_1, \cdots, a_n, b$, 若有

$$\exists u_1 v_1 w_1 \cdots u_n v_n w_n \Big(b = \prod_{1 \leqslant i \leqslant n} \big(a_i^{u_i} a_i^{v_i} a_i^{w_i}\big)\Big)$$

成立, 显见有

$$(a_1 = 1 \wedge \cdots \wedge a_n = 1) \to (b = 1)$$

成立．

(2.2) 另一方面，对任一群 $G$ 中任何元 $a_1,\cdots,a_n,b$. 若有

$$(a_1=1\wedge\cdots\wedge a_n=1)\to(b=1)$$

成立．以下再分二情况．

(2.2.1) 若 $b=1$. 仿 (1.2.1) 证法可知存在群 $H\supseteq G$ 及其中的元 $u_i,v_i,w_i$ 能使 $1=a_i^{u_i}a_i^{v_i}a_i^{w_i}$ $(i=1,\cdots,n)$. 从而有 $b=\prod\limits_{1\leqslant i\leqslant n}(a_i^{u_i}a_i^{v_i}a_i^{w_i})$.

(2.2.2) 若 $b\neq 1$. 此时 $a_1,\cdots,a_n$ 不全为 1, 不妨设 $a_1\neq 1$(其他情况仿此). 仿 (1.2.2) 可知存在 $H_1\supseteq G$ 及其中元 $u_1,v_1,w_1$ 能使 $b=a_1^{u_1}a_1^{v_1}a_1^{w_1}$. 又仿 (1.2.1) 知存在群 $H_2\supseteq H_1$ 及其中的元 $u_i,v_i,w_i$ 能使 $1=a_i^{u_i}a_i^{v_i}a_i^{w_i}$ $(i=2,\cdots,n)$. 从而在 $H_2$ 中有 $b=\prod\limits_{1\leqslant i\leqslant n}(a_i^{u_i}a_i^{v_i}a_i^{w_i})$.

由以上及定理 1 即知 $n>1$ 时引理也成立．　　(证毕)

**引理 2**　在群理论 $T$ 之下，对每一正整数 $n$, 令 $\overline{x}=(x_1,\cdots,x_n)$, $\overline{y}=(y_1,\cdots,y_n)$, 则下列公式集

$$\{t_i(\overline{x})=1\to t_i(\overline{y})=1\,|\,i=0,1,2,\cdots\}$$

(当 $i$ 通过一切自然数时， $t_i(\overline{x})$ 通过由 $\overline{x}$ 生成的一切项．) 等价于下列 $\exists_1$ 公式 $\varphi(\overline{x},\overline{y})$ 的结式:

$$\exists uv\Big(\bigwedge_{1\leqslant i\leqslant n}\Big(\bigwedge_{1\leqslant j\leqslant n}[x_i^u,y_j]=1\Big)\wedge\bigwedge_{1\leqslant i\leqslant n}x_i^v=x_i^u y_i\Big)$$

**证明**　(1) 一方面，对任一群 $G$ 中的任二 $n$ 元组 $\overline{a},\overline{b}$, 若有 $G\models\varphi(\overline{a},\overline{b})$, 则存在 $c,d\in G$ 能使诸 $[a_i^c,b_j]=1$ 及 $a_i^d=a_i^c b_i$. 此时，对任何项 $t_k(\overline{x})$, 易见有

$$(t_k(\overline{a}))^d=t_k(\overline{a}^d)=t_k(\overline{a}^c)t_k(\overline{b})=(t_k(\overline{a}))^c t_k(\overline{b}).$$

(其中 $\overline{a}^d=(a_1^d,\cdots,a_n^d)$, 其它仿此.) 由此易见有

$$G\models(t_k(\overline{a})=1\to t_k(\overline{b})=1),\ (k=0,1,2,\cdots).$$

(2) 另一方面，对任一群 $G$ 中的任二 $n$ 元组 $\overline{a},\overline{b}$, 若有

$$G\models(t_i(\overline{a})=1\to t_i(\overline{b})=1),\ (i=0,1,2,\cdots),$$

则易见存在一个同态映射 $\alpha:\langle\overline{a}\rangle_G\to\langle\overline{b}\rangle_G$ 使 $a_1\mapsto b_1,\cdots,a_n\mapsto b_n$.

现在在 $G$ 之外取一个与 $\langle\overline{a}\rangle_G$ 同构的群 $C$ 使以 $\overline{c}$ 为与 $\overline{a}$ 对应的生成元. 则由定理 3 知存在群 $H\supseteq G\times C$ 及其中的元 $g$ 适合 $a_i^g=c_i$ $(i=1,\cdots,n)$. 显见每个 $c_i$ 与每个 $b_j$ 可换. 由以上不难看出，由 $a_i\mapsto c_ib_i$ 可以决定一个由 $\langle\overline{a}\rangle_G$ 到 $H$ 内的同构映射，从而再由定理 3 可知存在群 $G'\supseteq H$ 及其中的元 $h$ 能使

$$a_i^h=c_ib_i=a_i^gb_i\ (i=1,\cdots,n).$$

由以上即知 $G'\models\varphi(\overline{a},\overline{b})$. (证毕)

**注** 以下有时把此引理中的 $\varphi(\overline{x},\overline{y})$ 改记为 $\mathrm{Hom}_n(\overline{x},\overline{y})$. 由上证中的 (1) 可以看出：若在一群 $G$ 中有 $\varphi(\overline{a},\overline{b})$ 成立，则由 $a_i\mapsto b_i$ $(i=1,\cdots,n)$ 可以决定一个由 $\langle\overline{a}\rangle_G$ 到 $\langle\overline{b}\rangle_G$ 的同态映射. 这就是记号 "$\mathrm{Hom}_n$" 的动机.

**定理 5** 设 $\mathcal{L}$ 及 $T$ 如上述. 若 $\Phi(\overline{x})$ 为 $\mathcal{L}$ 上递归可枚举的无量词严格 Horn 公式集，则存在 $\mathcal{L}$ 上的正原始公式 $\rho(\overline{x})$, 其在 $T$ 下的结式 $\mathrm{Res}_\rho(\overline{x})$ 与 $\Phi(\overline{x})$ 在 $T$ 下等价.

**证明** (1) 设 $\Phi(\overline{x})=\{\varphi_i(\overline{x})|\ i=0,1,2,\cdots\}$. 显见，对每个 $i$, 不妨设 $\varphi_i$ 为如下形状：

$$(t_{i1}(\overline{x})=1\wedge\cdots\wedge t_{im_i}(\overline{x})=1)\to(t_i(\overline{x})=1).$$

从而由引理 1 知 $\varphi_i$ 可视为一如下形状的公式 $\rho_i(\overline{x})$

$$\exists u_1v_1w_1\cdots u_{m_i}v_{m_i}w_{m_i}\Big(t_i(\overline{x})=\prod_{1\leqslant j\leqslant m_i}\big(t_{ij}(\overline{x})^{u_j}t_{ij}(\overline{x})^{v_j}t_{ij}(\overline{x})^{w_j}\big)\Big)$$

的结式. 为了方便, 以下设诸 $\rho_i(\overline{x})$ 中的约束变元都已改用 $v_1, v_2, v_3, \cdots$ 重写, 并且当 $i_1 \neq i_2$ 时在 $\rho_{i_1}(\overline{x})$ 及 $\rho_{i_2}(\overline{x})$ 中没有相同的约束变元. 我们以 $\psi_i$ 记 $\rho_i$ 中的无量词部分, 则由以上易见, 映射 $\varphi_i \mapsto \psi_i$ 是递归的.

现在引进两个新变元 $y, z$, 并把每个 $\psi_i$ 中的诸 $v_n$ 都各用 $[[y, z^{2n+1}], y]$ 代替 $(n = 1, 2, 3, \cdots)$. 则每个 $\psi_i$ 变为一无量词公式 $\sigma_i(\overline{x}, y, z)$, 并且映射 $\psi_i \mapsto \sigma_i$ 是递归的.

以 $\Psi(\overline{x}, y, z)$ 记在诸 $\sigma_i$ 中出现的等式的全集 (不妨设每个等式右端均为 1), 则由 $\Phi(\overline{x})$ 为递归可枚举及以上可知 $\Psi(\overline{x}, y, z)$ 也是递归可枚举的. 任意取定 $\Psi(\overline{x}, y, z)$ 中诸等式的一种递归枚举方式, 并对之改写为如下的等价形式: 把第 $n$ 个枚举出来的等式右端的 1 改写为 $n$ 个 $yy^{-1}$ 的连乘积. 以 $\Psi'(\overline{x}, y, z)$ 记这些新等式的全集, 则易见其为递归集.

现在考虑有限生成的群 $H = \langle \overline{x}, y, z; \Psi' \rangle$, 由定理 2 知 $H$ 可嵌入一个有限给出的群 $K$ 中. 任意取定 $K$ 的一种有限给出形式, 在此基础上并把 $\overline{x}, y, z$ 也都加入生成元中 (随之加入有限个必要的等式), 可以使 $K$ 具有形式 $\langle \overline{x}, y, z; \overline{w}; \Theta \rangle$, 其中 $\Theta(\overline{x}, y, z, \overline{w})$ 是一个含有限个等式的集合.

以 $\rho(\overline{x})$ 记下列公式 (易见为正原始公式):

$$\exists yz\overline{x'}y'z'\overline{w'}\Big(\bigwedge \Theta(\overline{x'}, y', z', \overline{w'}) \wedge \mathrm{Hom}_n(\overline{x'}, y', z'; \overline{x}, y, z)\Big)$$

其中 $n$ 为变元组 $\overline{x}, y, z$ 的长度.

(2) 以下证明 $\Phi(\overline{x})$ 等价于 $\rho(\overline{x})$ 在 $T$ 下的结式.

(2.1) 设 $G$ 为一群, 并且其中的元素组 $\overline{a}$ 适合 $G \vDash \rho(\overline{a})$, 则由 $\rho(\overline{x})$ 定义及 $\Theta$ 取法可知: 存在 $G$ 中的元素 $b, c$ 及 $\overline{a'}, b', c'$ 能使 $G \vDash \bigwedge \Psi'(\overline{a'}, b', c')$, 并且由 $\mathrm{Hom}_n$ 定义及引理 2 的证明可知, $\langle \overline{a}, b, c \rangle_G$(指由 $\overline{a}, b, c$ 在 $G$ 中生成的子群, 以下仿此) 是 $\langle \overline{a'}, b', c' \rangle_G$ 的同态象 (在一适当同态映射下, $\overline{a'}, b', c'$ 分别映射到 $\overline{a}, b, c$). 由

此可得 $G \vDash \bigwedge \Psi'(\overline{a}, b, c)$, 从而也有 $G \vDash \bigwedge \Psi(\overline{a}, b, c)$. 再由 $\Psi(\overline{x}, y, z)$ 的来历即易知有 $G \vDash \varphi_i(\overline{a})$ $(i = 0, 1, 2, \cdots)$.

由以上可知 $\Phi(\overline{x}) \subseteq \mathrm{Res}_\rho(\overline{x})$.

(2.2) 反之, 设 $G$ 及其中元素组 $\overline{a}$ 适合 $G \vDash \bigwedge \Phi(\overline{a})$.

由 $G \vDash \varphi_0(\overline{a})$ 及 $\varphi_0$ 为 $\rho_0$ 的结式可知 (由定理 1) $G$ 有扩群 $G_0$ 适合 $G_0 \vDash \rho_0(\overline{a})$; 又由 $G \vDash \varphi_1(\overline{a})$ 及 $\varphi_1$ 形状知 $G_0 \vDash \varphi_1(\overline{a})$, 故由 $\varphi_1$ 为 $\rho_1$ 的结式可知 $G_0$ 有扩群 $G_1$ 适合 $G_1 \vDash \rho_1(\overline{a})$; 如此继续, 可得 $G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots$.

令 $G_\omega = \bigcup_{i<\omega} G_i$($\omega$ 为第 1 个无限基数), 则有 $G_\omega \vDash \rho_i(\overline{a})$ $(i = 0, 1, 2, \cdots)$. 再由诸 $\psi_i$ 的取法可知, $G_\omega$ 中含有诸元素组 $\overline{d_0}, \overline{d_1}, \overline{d_2}, \cdots$ 能使 $G_\omega \vDash \psi_i(\overline{a}, \overline{d_i})$. 由此及诸 $\sigma_i$ 的取法及定理 4 可知, 存在群 $G' \supseteq G_\omega$ 及 $b, c \in G'$ 能使 $G' \vDash \sigma_i(\overline{a}, b, c)$ $(i = 0, 1, 2, \cdots)$.

由上段易见有 $G' \vDash \bigwedge \Psi'(\overline{a}, b, c)$. 由此及 $H$ 的定义可知 $\langle \overline{a}, b, c \rangle_{G'}$ 是 $H$ 的同态象. 由此及 $K = \langle \overline{x}, y, z, \overline{w}; \Theta \rangle$ 及 $\rho(\overline{x})$ 的形状 (注意 $\overline{x}$ 在 $\rho$ 中为自由变元而在 $K$ 中为一组生成元的一部分, 这两者不会混淆), 即易见在 $G$ 的扩群 $G'' = G' \times K$ 中有 $G'' \vDash \rho(\overline{a})$ 成立.

(2.3) 由 (2.1) 及 (2.2) 及定理 1 即易见: $\Phi(\overline{x})$ 与 $\mathrm{Res}_\rho(\overline{x})$ 在 $T$ 下等价. (证毕)

## §2 存在封闭群与群的字问题

以下把存在封闭群简称为 e.c. 群.

**引理 3** 设 $\mathcal{L} = \{\cdot, ^{-1}, 1\}$, $\varphi(\overline{x})$ 为 $\mathcal{L}$ 上的 $\exists_1$ 公式, $\overline{x} = (x_1, \cdots, x_n)$. 又设 $\overline{a}$ 为 e.c. 群 $G$ 中任一 $n$ 元组. 如果存在群 $H \supseteq G$ 适合 $H \vDash \varphi(\overline{a})$, 则 $G \vDash \varphi(\overline{a})$.

**证明** 设 $\varphi(\overline{x})$ 为 $\exists \overline{y} \psi(\overline{x}, \overline{y})$ ($\psi$ 中无量词). 不妨设 $\psi$ 已化为析取标准形 $\theta_1(\overline{x}, \overline{y}) \vee \cdots \vee \theta_k(\overline{x}, \overline{y})$ (其中每个 $\theta_i$ 为若干等式及不等

式的合取).

由 $H \models \varphi(\overline{a})$ 知存在 $\theta_i(1 \leqslant i \leqslant k)$ 能使 $H \models \exists\overline{y}\theta_i(\overline{a},\overline{y})$, 再由 $G$ 为 e.c. 群可知有 $G \models \exists\overline{y}\theta_i(\overline{a},\overline{y})$, 从而也有 $G \models \varphi(\overline{a})$. (证毕)

**定理 6** 设 $\mathcal{L},T$ 如前, $\varphi(\overline{x})$ 为 $\mathcal{L}$ 上的 $\exists_1$ 公式, $\overline{x}=(x_1,\cdots,x_n)$. 又设 $G$ 为一 e.c. 群, $\overline{a}$ 为其中任一 $n$ 元组. 则 $G \models \varphi(\overline{a})$ 当且仅当 $G \models \bigwedge \mathrm{Res}_{\varphi}(\overline{a})$.

**证明** (1) 若 $G \models \varphi(\overline{a})$, 则由 $\mathrm{Res}_{\varphi}(\overline{x})$ 定义易见有 $G \models \bigwedge \mathrm{Res}_{\varphi}(\overline{a})$.

(2) 反之, 若 $G \models \bigwedge \mathrm{Res}_{\varphi}(\overline{a})$, 则由定理 1 知存在群 $H \supseteq G$ 适合 $H \models \varphi(\overline{a})$, 再由引理 3 即知 $G \models \varphi(\overline{a})$.

**定理 7** 每个群 $G$ 都能扩张为一 e.c. 群.

这一定理虽很基本, 但以下并未用到, 所以略去证明. 读者可参看 [4] 中定理 3.10 的证法, 其思路与将任一域扩张为一代数闭域的过程类似.

**定理 8** 每个 e.c. 群 $G$ 都是单群.

**证明** 任取 $G$ 中二元 $a \neq 1$ 及 $b \neq 1$.

在 $G$ 之外取一个与 $\langle a\rangle_G$ 同构的循环群 $C$, 设 $c$ 为其一生成元. 考虑自由积 $G * C$. 由自由积性质 (可参看 [7] 第 11 章) 可知 $ca$ 与 $c^{-1}b$ 均为周期无限. 故由定理 3 可知, 存在一群 $H \supseteq G * C$ 及其中二元 $u,v$ 能使 $a^u = c$ 及 $(ca)^v = c^{-1}b$. 从而易见在 $H$ 中有 $b = a^u a^{uv} a^v$. 所以

$$H \models \exists xy(b = a^x a^{xy} a^y),$$

再由 $H \supseteq G$ 及 $G$ 为 e.c. 群知 $G$ 也适合此式, 故知存在 $h,k \in G$ 能使 $b = a^h a^{hk} a^k$. 由此可知: $b$ 属于 $a$ 在 $G$ 中生成的正规子群.

由 $a,b$ 的任意性及以上所述即知 $G$ 为单群. (证毕)

**定义** 设 $H$ 为一有限生成的群, 以 $\overline{h}=(h_1,\cdots,h_n)$ 为一组生成元. 取变元组 $\overline{x}=(x_1,\cdots,x_n)$(诸 $x_i$ 互异). 现在把语言 $\mathcal{L}=\{\cdot,^{-1},1\}$ 上由 $x_1,\cdots,x_n$ 所构成的一切项任依一种递归方式排列

为：

$$t_0(\overline{x}), t_1(\overline{x}), t_2(\overline{x}), \cdots$$

(易见此为可能). 并令

$$I_{\overline{h}} = \{i|\ H \models t_i(\overline{h}) = 1\},$$

我们把 $I_{\overline{h}}$ 称为群 $H$ 在生成元组 $\overline{h}$ 下的 **字问题**. (注意：上述的 $I_{\overline{h}}$ 虽与诸 $t_i(\overline{x})$ 的递归排列方式有关，但易知其在递归论意义下的不可解度与递归排列方式无关. 另外，当 $H$ 的生成元组 $\overline{h}$ 改变时，虽然 $I_{\overline{h}}$ 也随之改变，但易知其不可解度也不变. 我们把此不可解度记为 $d_H$.)

当 $d_H$ 为递归集的度 (一般记为 0) 时，称 $H$ 的字问题 **递归可解**. 当 $d_H$ 为一递归可枚举集的度时，称 $H$ 有 **递归可枚举** 的字问题.

**定理 9** 设 $H$ 为一有限生成的群，其字问题递归可解. 则 $H$ 可以嵌入每一 e.c. 群 $G$ 中.

**证明** 易知 $G \neq \{1\}$. 任意取定 $G$ 中一个元 $g \neq 1$, 则 $G$ 中每一不等式 $s \neq t$ 都可等价地改写为 $(s = t \to g = 1)$ 形状.

取 $H$ 的一组生成元 $\overline{a} = (a_1, \cdots, a_n)$. 对于此 $n$, 把 $\mathcal{L}$ 上由互异变元 $x_1, \cdots, x_n$ 组成的一切项任依一递归方式排列为 $t_0(\overline{x}), t_1(\overline{x})$, $t_2(\overline{x}), \cdots$. 并令

$$X^+ = \{i|\ H \models t_i(\overline{a}) = 1\}.$$

由 $H$ 取法可知 $X^+$ 与 $X^- = \omega \setminus X^+$ ($\omega$ 为自然数集) 均为递归集. 再令 $\Phi(\overline{x}, z)$ 为 $\mathcal{L}$ 上如下的公式集：

$$\{t_i(\overline{x}) = 1|\ i \in X^+\} \cup \{t_i(\overline{x}) = 1 \to z = 1|\ i \in X^-\}.$$

易见 $\Phi(\overline{x}, z)$ 为 $\mathcal{L}$ 上递归的无量词严格 Horn 公式集，故由定理 5 知存在 $\mathcal{L}$ 上的正原始公式 $\varphi(\overline{x}, z)$ 以 $\Phi(\overline{x}, z)$ 为结式.

由以上易见 $G\times H\vDash\bigwedge\Phi(\overline{a},g)$. 再由上段及定理 1 知存在群 $G'\supseteq G\times H$ 能使 $G'\vDash\varphi(\overline{a},g)$, 从而有

$$G'\vDash\exists\overline{x}z(\varphi(\overline{x},z)\wedge z\neq 1),$$

再由 $G'\supseteq G$ 及 $G$ 为 e.c. 群知 $G$ 也适合此式, 所以存在 $\overline{b},h\in G$ 能使 $G\vDash\varphi(\overline{b},h)$ 且 $h\neq 1$, 从而由上段知 $G\vDash\bigwedge\Phi(\overline{b},h)$. 再由 $\Phi(\overline{x},z)$ 的定义即易见 $\overline{b}$ 在 $G$ 中生成的子群 $\langle\overline{b}\rangle_G$ 与 $H$ 同构. (证毕)

**推论** 设 $H$ 为一有限生成的群, 其字问题递归可枚举, 则存在 $\mathcal{L}$ 上一个 $\exists_3$ 语句 $\sigma_H$ 能适合: 对每一 e.c. 群 $G$, $G\vDash\sigma_H$ 当且只当 $H$ 能嵌入 $G$ 中.

**证明** 任取一 e.c. 群 $G$, 现在利用 $G$ 寻找 $\sigma_H$. (由以下关于 $\sigma_H$ 的构作可看出, $\sigma_H$ 实际与 e.c. 群 $G$ 的取法无关.)

显见无限循环群 $C$ 的字问题递归可解, 故由定理 9 知 $C$ 可嵌入 $G$ 中, 所以 $G$ 含有周期无限的元素, 任意取定其一为 $g$. 令 $\mathcal{L}_g=\mathcal{L}\cup\{c_g\}$ ($c_g$ 为一新常量), 并视 $(G,g)$ 为 $\mathcal{L}_g$ 的模型 (以 $g$ 作为 $c_g$ 的解释), 记为 $G_g$. (显见 $G_g$ 仍为 e.c. 群.)

考虑 $\mathcal{L}$ 上的递归公式集

$$\Phi_1(x,y,z)=\{y=x^n\to z=1\mid n=0,1,2,\cdots\}.$$

由 $\Phi_1$ 中诸公式形状及定理 5 与定理 6 可知存在 $\mathcal{L}$ 上的正原始公式 $\varphi(x,y,z)$, 它在 e.c. 群 $G$ 中与 $\Phi_1$ 中公式的合取等价. 从而易见 $\neg\varphi(c_g,y,c_g)$ 在 $G_g$ 中与 "$y$ 为某一 $g^n(n\geqslant 0)$" 等价. $\neg\varphi(c_g,y,c_g)$ 可以逻辑等价地化为一 $\forall_1$- 公式, 记为 $N(y,c_g)$.

设 $R$ 为 $\omega$ 的任一递归可枚举子集. 考虑公式集

$$\Phi_2(x,y,z)=\{y=x^m\to z=1\mid m\in R\}.$$

仿照上段, 利用定理 5 与定理 6, 并经过对公式取否定形式, 可得 $\mathcal{L}_g$ 上一 $\forall_1$ 公式 $\theta_R(y,c_g)$ 使得:

(i) 对一切自然数 $m$: $m \in R$ 当且只当 $G_g \models \theta_R(c_g^m, c_g)$.

由题设知，存在 $H$ 的一组生成元 $\overline{a} = (a_1, \cdots, a_n)$ 能使 $R_1 = \{i \mid H \models t_i(\overline{a}) = 1\}$ 为递归可枚举集 ($t_i$ 的含义见字问题定义). 考虑下列的 (无限长) 公式:

(ii) $\forall y(N(y, c_g) \wedge \theta_{R_1}(y, c_g) \to \bigwedge\limits_{i<\omega} (y = c_g^i \to t_i(\overline{x}) = 1))$

$\wedge \forall y(N(y, c_g) \wedge \neg\theta_{R_1}(y, c_g) \to \bigwedge\limits_{i<\omega} (y = c_g^i \wedge t_i(\overline{x}) = 1 \to c_g = 1))$.

由以上可知，对 $G$ 中任一 $n$ 元组 $\overline{b}$: "(ii) 式在 $G_g$ 中对 $\overline{b}$ 成立" 当且只当 "对每个自然数 $i$, $t_i(\overline{b}) = 1$ 当且只当 $i \in R_1$" 当且只当 "$\overline{b}$ 在 $G_g$ 中生成的子群能通过 $b_i \mapsto a_i$ $(i = 1, \cdots, n)$ 得出到 $H$ 上的同态映射".

以下把 (ii) 进行简化:

用定理 5 两次，可以用两个 $\exists_1$ 公式代换 (ii) 中的两个无限合取式，得到一个 $\mathcal{L}_g$ 上的 1 阶公式 $\sigma'(\overline{x}, c_g)$. 再由 $g$ 的周期无限及以上讨论可知 (以下又回到 $\mathcal{L}$ 上):

(iii) "$H$ 可嵌入 $G$ 中" 当且只当 "$G \models \exists\overline{x}z((z$周期无限$) \wedge \sigma'(\overline{x}, z))$".

而 "$z$ 周期无限" 又可表示为

(iv) $\exists w\Big(w \neq 1 \wedge \bigwedge\limits_{i>0} (z^i = 1 \to w = 1)\Big)$. 再次用定理 5, 可把 (iv) 化为一 $\exists_1$ 公式 $I(z)$.

现在令 $\sigma''_H$ 为

$$\exists\overline{x}z(I(z) \wedge \sigma'(\overline{x}, z)),$$

则由以上易知 $\sigma''_H$ 逻辑等价于一个 $\exists_3$ 语句 $\sigma_H$. 显见 $\sigma_H$ 与 $G$ 的取法无关，并且具有推论中所说的性质. (证毕)

## §3 模型论力迫法

**定义** 设 $T$ 为语言 $\mathcal{L}$ 上的一集原子语句，若适合下列二条件，则称 $T$ 为 **对等号封闭** 的：

(i) 对 $\mathcal{L}$ 上每一闭项 (即不含变元的项)$t$，都有 $(t=t)\in T$.

(ii) 对 $\mathcal{L}$ 上每一原子公式 $\varphi(\overline{x})$ 及任二闭项 $s,t$，若 $\varphi(s)\in T$ 并且 "$(s=t)\in T$ 或 $(t=s)\in T$"，则 $\varphi(t)\in T$.

**定理 10**(典型模型定理) 设 $\mathcal{L}$ 为一语言，其中至少含 1 个常量符号. $T$ 为 $\mathcal{L}$ 上一集原子语句，对等号封闭. 则存在 $\mathcal{L}$ 的模型 $A$ 适合下列二条件：

(a) $A$ 中每一元都是 $\mathcal{L}$ 上一个闭项 $t$ 的解释 $t^A$.

(b) 对 $\mathcal{L}$ 上每一原子语句 $\varphi$，$A\vDash\varphi$ 当且只当 $\varphi\in T$.

并且，此种 $A$ 除同构外唯一 (以下称为 $T$ 的典型模型).

**证明** 以下只简述其证法大意，详细论证可参看 [4] 中引理 2.2 的证明.

(1) 以 $K$ 记 $\mathcal{L}$ 上全体闭项所成的集. 在 $K$ 上定义一关系 "$\sim$" 如下：

$$s\sim t \text{ 当且只当 } (s=t)\in T.$$

由 $T$ 对等号封闭可知 "$\sim$" 是 $K$ 上的等价关系. 以 $t^\sim$ 记 $t$ 所在的等价类.

我们取 $\{t^\sim\mid t\in K\}$ 作为模型 $A$ 的论域 $\mathrm{dom}(A)$ (由 $\mathcal{L}$ 含常量符号知 $\mathrm{dom}(A)$ 不空.)

对 $\mathcal{L}$ 中每一常量符号 $c$，在 $\mathrm{dom}(A)$ 中取 $c^\sim$ 作为 $c$ 在 $A$ 中的解释 $c^A$.

对 $\mathcal{L}$ 中每一 $n$ 元 $(n\geqslant 1)$ 函数符号 $F$，在 $\mathrm{dom}(A)$ 上如下定义一 $n$ 元函数作为 $F$ 在 $A$ 中的解释 $F^A$:

$$F^A(t_1^\sim,\cdots,t_n^\sim)=(F(t_1,\cdots,t_n))^\sim.$$

(由 $T$ 对等号封闭可知此定义合理.)

对 $\mathcal{L}$ 中每一 $n$ 元 $(n \geqslant 1)$ 关系符号 $R$, 在 $\mathrm{dom}(A)$ 上如下定义一 $n$ 元关系作为 $R$ 在 $A$ 中的解释 $R^A$:

$$(t_1^{\sim}, \cdots, t_n^{\sim}) \in R^A \text{ 当且只当 } R(t_1, \cdots, t_n) \in T.$$

(由 $T$ 对等号封闭可知此定义合理.)

模型 $A$ 的定义至此完成.

对于 $K$ 中每一闭项 $t$, 可按其复杂性归纳证明有 $t^A = t^{\sim}$. 由此即易知 (a) 及 (b) 成立.

(2) 此外还可证明, $A$ 适合下列性质:

(c) 对 $T$ 的每一模型 $B$, 都存在唯一的同态映射 $f: A \to B$.

由 (c) 即易知: 若又有 $\mathcal{L}$ 的模型 $A_1$ 也适合 (a) 及 (b), 则 $A_1$ 与 $A$ 同构. (证毕)

设 $\mathcal{L}$ 为一可数语言, $T$ 为 $\mathcal{L}$ 上的和谐理论. 令 $\mathcal{L}(W) = \mathcal{L} \cup W$, 其中 $W$ 为一可数无限的新常量集. ($W$ 中的常量以下称为"见证".)

设 $p$ 是由 $\mathcal{L}(W)$ 中有限个原子语句或原子语句的否定所成的集合. 如果 $T \cup p$ 和谐, 则称 $p$ 是一个 **T- 条件**. (注意: 空集是 $T$-条件.)

设 $P$ 是关于 $\mathcal{L}(W)$ 的模型的一个性质, 考虑下列的博奕 $G(P)$: 有奕手甲、乙二人. 先由甲选取一个 $T$- 条件 $p_0$; 再由乙选取一个 $T$- 条件 $p_1$ 使 $p_0 \subseteq p_1$; 再由甲选取一个 $T$- 条件 $p_2$ 使 $p_1 \subseteq p_2$; 再由乙选取一个 $T$- 条件 $p_3$ 使 $p_2 \subseteq p_3$; $\cdots\cdots$ 如此继续, 可得 $T$- 条件的一个可数无限递增列:

$$p_0 \subseteq p_1 \subseteq p_2 \subseteq p_3 \subseteq \cdots.$$

令 $\bar{p} = \bigcup_{i<\omega} p_i$. 现在取 $\bar{p}$ 中一切原子语句所成的集 $U_1$, 则易知存在唯一个最小的包括 $U_1$ 并且对等号封闭的原子语句集 $U$. 由定理 10

知 $U$ 有唯一的典型模型，记为 $A^+(\overline{p})$ 或 $A^+$，并将其在 $\mathcal{L}$ 上的归约记为 $A(\overline{p})$ 或 $A$. 如果 $A^+(\overline{p})$ 具有性质 $P$，则称乙获胜，否则称甲获胜.

如果乙对于 $G(P)$ 具有必胜策略，则称性质 $P$ 是 **可力迫的**. 而通过上述博奕来造 $\overline{p}$ 并由之得到 $A^+(\overline{p})$ 及 $A(p)$ 的过程，以下简称为 "**$T$- 力迫法**". (它是 A. Robinson 提出的 "模型论有限力迫法" 的一种形式.)

**引理 4**(可力迫性的联合引理) 在 $T$- 力迫法之下，如果诸性质 $P_i$ $(i=0,1,2,\cdots)$ 都是可力迫的，则性质 $\bigwedge\limits_{i<\omega} P_i$ (即：$P_0$ 且 $P_1$ 且 $P_2$ 且 $\cdots$) 也是可力迫的.

**证明** 由题设，乙对于每个博奕 $G(P_i)$ 都有一必胜策略 $\sigma_i$. 现在考虑博奕 $G(Q)$，其中 $Q=\bigwedge\limits_{i<\omega} P_i$. 在 $G(Q)$ 中，乙可以如下去走：

第 0,2,4,$\cdots$ 步为甲所走.

$$\begin{cases} \text{在第 } 1,5,9,13,\cdots \text{ 步，乙按策略 } \sigma_0 \text{ 走;} \\ \text{在第 } 3,11,19,27,\cdots \text{ 步，乙按策略 } \sigma_1 \text{ 走;} \\ \cdots\cdots \\ \text{在第 } 2^{k+1}-1, 2^{k+1}\cdot 3-1, 2^{k+1}\cdot 5-1, 2^{k+1}\cdot 7-1,\cdots \text{ 步,} \\ \qquad \text{乙按策略 } \sigma_k \text{ 走;} \\ \cdots\cdots \end{cases}$$

易见乙即能获胜. 所以这就是乙对于 $G(Q)$ 的一种必胜策略.

(证毕)

**定义** 设 $q$ 为一 $T$- 条件. 如果在前述的博奕 $G(P)$ 中，只要出现了某个 $p_i$ 能适合 $p_i \supseteq q$，乙此后对 $G(P)$ 就有了必胜策略. 则称 $T$- 条件 $q$ 能力迫性质 $P$，简称为 $q$ **力迫** $P$.

**引理 5** 在 $T$- 力迫法之下，如果 $T$- 条件 $q$ 能力迫诸性质 $P_i$

($i=0,1,2,\cdots$), 则 $q$ 也能力迫 $\bigwedge_{i<\omega} P_i$.

证明仿引理 4 者，略去.

**引理 6** 在 $T$- 力迫法中，有 $A^+(\overline{p})\vDash\overline{p}$.

**证明** 任取 $\varphi\in\overline{p}=\bigcup_{i<\omega}p_i$, 则由 $T$- 条件定义知 $\varphi$ 或为原子语句或为原子语句的否定.

(1) 若 $\varphi$ 为原子语句，则 (按前面定义 $A^+(\overline{p})$ 时的记号) $\varphi\in U_1\subseteq U$. 故由定理 10 的 (b) 知 $U$ 的典型模型 $A^+(\overline{p})\vDash\varphi$.

(2) 若 $\varphi$ 为 $\neg\sigma$ 形 ($\sigma$ 为原子语句).

假若 $A^+(\overline{p})\vDash\sigma$, 则由定理 10 的 (b) 知 $\sigma\in U$.

另一方面：由 $T$- 条件定义及紧致性定理可知 $\overline{p}$ 有模型 $B$. 由 $U_1\subseteq\overline{p}$ 知 $B\vDash U_1$, 由此及 $U$ 的定义易知也有 $B\vDash U$, 从而由以上的 $\sigma\in U$ 有 $B\vDash\sigma$. 但由 $\varphi\in\overline{p}$ 又有 $B\vDash\varphi$, 即 $B\vDash\neg\sigma$. 故得矛盾.

所以 $A^+(\overline{p})\vDash\sigma$ 不成立，从而有 $A^+(\overline{p})\vDash\varphi$. (证毕)

**引理 7** 在 $T$- 力迫法中，下列性质 $P$ 是可力迫的.

$P$: $A^+(\overline{p})$ 中每一元素都被无限多个见证所指称.

**证明** 在博奕 $G(P)$ 中，令乙按下列策略走，易见即能获胜. (设见证集 $W=\{c_1,c_2,c_3,\cdots\}$.)

在第 $i$ 步时 ($i=1,3,5,\cdots$): 设甲已走出的 $p_{i-1}$ 中所出现的全体见证都在 $c_1,c_2,\cdots,c_{n_i}$ 之中. (不妨设 $n_1>0$, 从而按乙的下列走法，可使每 $n_i>0$.)

现在令乙取

$$p_i=p_{i-1}\cup\{c_1=c_{n_i+1},c_2=c_{n_i+2},\cdots,c_{n_i+n_i}\}$$

即可 (易见 $p_i$ 为一 $T$- 条件). (证毕)

(注：上述性质 $P$ 也可被任何 $T$- 条件 $q$ 力迫. 证法类似.)

**引理 8** 设 $q$ 为一 $T$- 条件， $P$ 为关于 $\mathcal{L}(W)$ 的模型的一个性质. 如果对每一 $T$- 条件 $p \supseteq q$ 都存在一 $T$- 条件 $r \supseteq p$ 能使 $r$ 力迫 $P$. 则 $q$ 即能力迫 $P$.

证明略去 (由 T- 力迫定义易见).

**引理 9** 设 $q$ 为一 $T$- 条件， $\varphi$ 为 $\mathcal{L}(W)$ 上一个语句. 则 $q$ 力迫 $\neg\varphi$(指： $q$ 力迫 "$A^+(\overline{p}) \models \neg\varphi$". 以下仿此) 的充分必要条件是：不存在 $T$- 条件 $p \supseteq q$ 能使 $p$ 力迫 $\varphi$.

**证明** (1) 必要性. 设 $q$ 力迫 $\neg\varphi$. 则易见任何 $p \supseteq q$ 也力迫 $\neg\varphi$. 假若存在 $T$- 条件 $p_1 \supseteq q$ 能使 $p_1$ 力迫 $\varphi$, 则由引理 5 知 $p_1$ 力迫 $\varphi \wedge \neg\varphi$. 此显见不可能.

(2) 充分性. (2.1) 先证明：

(a) 若 $\varphi$ 为 $\mathcal{L}(W)$ 上一个原子语句， $p$ 为一 $T$- 条件，则 $p$ 力迫 $\neg\varphi$ 当且只当不存在 $T$- 条件 $r \supseteq p$ 能使 $\varphi \in r$.

(2.1.1) 若存在 $T$- 条件 $r \supseteq p$ 能使 $\varphi \in r$, 则易知 $r$ 能力迫 $\varphi$. 此时易见 $r$ 不能力迫 $\neg\varphi$. 从而 $p \subsetneq r$ 也不能力迫 $\neg\varphi$.

(2.1.2) 若不存在 $T$- 条件 $r \supseteq p$ 能使 $\varphi \in r$. 考虑博奕 $G(\neg\varphi)$. 不难看出，奕手乙有策略可以迫使 $\overline{p}$ 中全体原子语句所成的集 $U$ 对等号封闭，从而使 $A^+(\overline{p}) \models \varphi$ 当且只当 $\varphi \in U$(因 $A^+(\overline{p})$ 是 $U$ 的典型模型). 但若奕手甲走出某 $p_i \supseteq p$ 之后，则由本情况的题设易见 $\varphi \notin \overline{p}$, 所以 $\varphi \notin U$, 从而有 $A^+(\overline{p}) \models \neg\varphi$. 由以上即知 $p$ 力迫 $\neg\varphi$.

(2.2) 再证明：

(b) 对每一 $T$- 条件 $q$ 及 $\mathcal{L}(W)$ 上每一语句 $\varphi$, 或存在 $T$- 条件 $p \supseteq q$ 能力迫 $\varphi$, 或存在 $T$- 条件 $p \supseteq q$ 能力迫 $\neg\varphi$.

对 $\varphi$ 的复杂性归纳证明.

(2.2.1) 当 $\varphi$ 为原子语句时. 如果不存在 $T$- 条件 $p \supseteq q$ 能力迫 $\neg\varphi$. 则对任何 $T$- 条件 $p \supseteq q$, 由 (a) 知存在 $T$- 条件 $r \supseteq p$ 能使 $\varphi \in r$, 从而易见 $r$ 力迫 $\varphi$. 再由引理 8 即知 $q$ 力迫 $\varphi$. 所以此时 (b) 成立.

(2.2.2) 设对于 $\psi$ 已有 (b) 成立，当 $\varphi$ 为 $\neg\psi$ 形状时. 易见对于 $\varphi$ 也有 (b) 成立. （注意 $p$ 力迫 $\psi$ 当且只当 $p$ 力迫 $\neg\neg\psi$.)

(2.2.3) 设对于 $\varphi_1, \varphi_2$ 已有 (b) 成立，当 $\varphi$ 为 $\varphi_1 \wedge \varphi_2$ 形状时. 如果不存在 $T$- 条件 $p \supseteq q$ 能力迫 $\neg\varphi$, 则显见也不存在 $p \supseteq q$ 能力迫 $\neg\varphi_1$, 故由归纳假设可知对任何 $p \supseteq q$ 都存在 $r \supseteq p$ 能力迫 $\varphi_1$, 再由引理 8 即知 $q$ 力迫 $\varphi_1$. 同理知 $q$ 力迫 $\varphi_2$. 从而由引理 5 知 $q$ 力迫 $\varphi$.

(2.2.4) 设对于 $\psi(\overline{x})$ 及每一组见证 $\overline{c}$, 都已有关于 $\psi(\overline{c})$ 的 (b) 成立，当 $\varphi$ 为 $\forall\overline{x}\psi(\overline{x})$ 形状时，如果不存在 $T$- 条件 $p \supseteq q$ 能力迫 $\neg\varphi$, 则易见也不存在 $p \supseteq q$ 能力迫任何一个 $\neg\psi(\overline{c})$, 再仿 (2.2.3) 可知 $q$ 能力迫每个 $\psi(\overline{c})$. 现在考虑博奕 $G(\forall\overline{x}\psi(\overline{x}))$. 如果甲走出了任何包括 $q$ 的 $T$- 条件，则乙可以迫使最后造出的模型 $A^+(\overline{p})$ 中每一元素都被一见证所指称 (见引理 7 后面的注), 并且 (由以上及引理 5) 使每个 $\psi(\overline{c})$ 都在 $A^+(\overline{p})$ 中成立. 从而易见有 $A^+(\overline{p}) \models \varphi$. 所以 $q$ 力迫 $\varphi$.

(2.3) 现在证条件的充分性.

设不存在 $T$- 条件 $p \supseteq q$ 能力迫 $\varphi$. 则显见对任何 $p \supseteq q$, 也不存在 $r \supseteq p$ 能力迫 $\varphi$, 从而由 (b) 知存在 $r \supseteq p$ 能力迫 $\neg\varphi$. 再由引理 8 即知 $q$ 力迫 $\neg\varphi$. (证毕)

**引理 10** 设 $T$ 为可数语言 $\mathcal{L}$ 上的 $\forall_1$ 理论，则“所造的模型 $A$ 适合 $A \models T$”这一性质是可力迫的.

**证明** (1) 任取 $T$ 中一语句 $\forall\overline{x}\psi(\overline{x})$ ($\psi$ 中无量词).

(1.1) 现在证明：对任一组见证 $\overline{c}$, $\psi(\overline{c})$ 都是可力迫的.

在博奕 $G(\psi(\overline{c}))$ 中，设甲走出了 $T$- 条件 $p_0$. 显见 $T \vdash \psi(\overline{c})$, 再由 $T \cup p_0$ 和谐可知 $T \cup p_0 \cup \{\psi(\overline{c})\}$ 有一模型 $B$. 把 $\psi(\overline{c})$ 表示为析取标准形 $\bigvee\limits_{1\leqslant i\leqslant m}\Big(\bigwedge\limits_{1\leqslant j\leqslant n_i}\theta_{ij}\Big)$, 则存在 $i$ 能使 $B \models \bigwedge\limits_{1\leqslant j\leqslant n_i}\theta_{ij}$. 任意取定一个这样的 $i$, 并令 $q = p_0 \cup \{\theta_{i1}, \cdots, \theta_{in_i}\}$, 则易见 $q$ 为 $T$- 条

件，所以乙可以走出 $p_1 = q$. 由此及引理 6 即知有 $A^+(\overline{p}) \vDash q$, 从而由 $q$ 的取法可知 $A^+(\overline{p}) \vDash \psi(\overline{c})$.

(1.2) 由 (1.1) 及引理 7 和引理 4 可知乙又可 (在另一策略下) 迫使 $A^+(\overline{p}) \vDash \forall \overline{x} \psi(\overline{x})$.

(2) 由 $\mathcal{L}$ 可数知 $T$ 可数. 再由 (1) 及引理 4 即可得引理的结论.　　(证毕)

(注：对于 $\mathcal{L}$ 上的 $\forall_2$ 理论 $T$, 本引理也成立，但以下无用.)

**引理 11**　设 $q$ 为一 $T$- 条件， $\psi(x_1, \cdots, x_n)$ 为 $\mathcal{L}(W)$ 上一个公式， $c_1, \cdots, c_n$ 为一组不出现于 $q$ 及 $\psi$ 中的互异见证. 如果 $q$ 力迫 $\psi(c_1, \cdots, c_n)$, 则 $q$ 也力迫 $\forall x_1 \cdots x_n \psi(x_1, \cdots, x_n)$.

**证明**　设 $q$ 力迫 $\psi(c_1, \cdots, c_n)$.

(1) 任取一组见证 $d_1, \cdots, d_n$(不论同异). 现在证明 $q$ 力迫 $\psi(d_1, \cdots, d_n)$.

任取 $T$- 条件 $p \supseteq q$. 再任取一组不出现于 $p$ 及 $\psi(d_1, \cdots, d_n)$ 中的互异见证 $c_1', \cdots, c_n'$. 由于 $c_1, \cdots, c_n$ 及 $c_1', \cdots, c_n'$ 各是一组不出现于 $q$ 及 $\psi(x_1, \cdots, x_n)$ 中的互异见证并且由题设知 $q$ 力迫 $\psi(c_1, \cdots, c_n)$, 故由 $T$- 条件定义及力迫过程易见 $q$ 也能力迫 $\psi(c_1', \cdots, c_n')$.

令 $r = p \cup \{c_1' = d_1, \cdots, c_n' = d_n\}$, 由 $c_1', \cdots, c_n'$ 取法易知 $r$ 为 $T$- 条件. 并且由 $r \supseteq q$ 及上段可知 $r$ 能力迫 $\psi(c_1', \cdots, c_n')$, 再由 $r$ 的定义即知 $r$ 能力迫 $\psi(d_1, \cdots, d_n)$.

由以上及引理 8 即知 $q$ 力迫 $\psi(d_1, \cdots, d_n)$.

(2) 由 (1) 及引理 7 的注及引理 5, 即不难证明本引理的结论. (可参看引理 9 证明中 (2.2.4)).　　(证毕)

**引理 12**　设 $p$ 为一 $T$- 条件， $\varphi$ 为 $\mathcal{L}(W)$ 上一个 $\exists_1$ 语句. 若 $T \cup p \cup \{\varphi\}$ 和谐，则存在 $T$- 条件 $q \supseteq p$ 能使 $q \vdash \varphi$.

**证明**　设 $\varphi$ 为 $\exists \overline{x} \psi(\overline{x})$ ($\psi(\overline{x})$ 中无量词). 任取一组不在 $p$ 及 $\varphi$ 中出现的互异见证 $\overline{c}$, 则由题设可知 $T \cup p \cup \{\psi(\overline{c})\}$ 和谐，任取其一

模型 $B$. 把 $\psi(\overline{c})$ 表示为析取标准形 $\bigvee_{1\leqslant i\leqslant m}\Big(\bigwedge_{1\leqslant j\leqslant n_i}\theta_{ij}\Big)$, 则对某个 $i$ 有 $B\vDash\bigwedge_{1\leqslant j\leqslant n_i}\theta_{ij}$. 对于此 $i$, 令

$$q=p\cup\{\theta_{i1},\cdots,\theta_{in_i}\},$$

则 $B\vDash T\cup q$. 所以 $q$ 是一 $T$- 条件. 显见 $q\supseteq p$ 并且有 $q\vdash\psi(\overline{c})$ 及 $q\vdash\varphi$. (证毕)

**定理 11** 设 $p$ 为一 $T$- 条件, $\psi(\overline{x})$ 为 $\mathcal{L}(W)$ 上一个无量词公式. 如果 $p$ 力迫 $\forall\overline{x}\psi(\overline{x})$, 则 $T\cup p\vdash\forall\overline{x}\psi(\overline{x})$. (反之, 若有 $T\cup p\vdash\forall\overline{x}\psi(\overline{x})$, 则也有 $p$ 力迫 $\forall\overline{x}\psi(\overline{x})$, 但此事以下无用.)

**证明** 任取一组不出现于 $p$ 及 $\psi$ 中的互异见证 $\overline{c}$. 现在证 $T\cup p\vdash\psi(\overline{c})$. (从而即有 $T\cup p\vdash\forall\overline{x}\psi(\overline{x})$).

假若

$$T\cup p\nvdash\psi(\overline{c}). \tag{1}$$

则 $T\cup p\cup\{\neg\psi(\overline{c})\}$ 和谐, 从而由引理 12 知存在 $T$- 条件 $q\supseteq p$ 能使 $q\vdash\neg\psi(\overline{c})$. 此时, 在博奕 $G(\psi(\overline{c}))$ 中, 若甲走出 $p_0=q$, 则由引理, 有 $A^+(\overline{p})\vDash q$, 从而 $A^+(\overline{p})\vDash\neg\psi(\overline{c})$, 乙不能胜此博奕. 这说明, 若 (1) 式成立, 则 $p$ 不力迫 $\psi(\overline{c})$, 从而易见 $p$ 不力迫 $\forall\overline{x}\psi(\overline{x})$, 与题设矛盾. (证毕)

## §4 各种存在封闭群的存在性

**定理 12** 设 $T$ 为语言 $\mathcal{L}$ 上的理论. 则下列二条件等价:

(a) $A$ 是 $T$ 的存在封闭模型 (简称 e.c. 模型).

(b) $A$ 是 $T$ 的模型, 并且对 $\mathcal{L}$ 上每一 $\exists_1$ 公式 $\varphi(\overline{x})$ 都有

$$A\vDash\forall\overline{x}(\bigwedge\mathrm{Res}_\varphi(\overline{x})\to\varphi(\overline{x})).$$

(注: $T$ 的 e.c. 模型与 e.c. 群的定义类似, 在此略去.)

**证明** (1) 由 (a) 证 (b).

任取 $\mathcal{L}$ 上 $\exists_1$ 公式 $\varphi(\overline{x})$. 设 $A$ 中元素组 $\overline{a}$ 适合 $A \vDash \bigwedge \mathrm{Res}_{\varphi}(\overline{a})$. 现在证 $A \vDash \varphi(\overline{a})$.

由定理 1 知存在 $T$ 的模型 $B \supseteq A$ 能使 $B \vDash \varphi(\overline{a})$. 再由 $A$ 为 $T$ 的 e.c. 模型即知 $A \vDash \varphi(\overline{a})$.

(2) 由 (b) 证 (a).

任取 $\mathcal{L}$ 上 $\exists_1$ 公式 $\varphi(\overline{x})$ 及 $A$ 中元素组 $\overline{a}$. 若存在 $T$ 的模型 $B \supseteq A$ 能使 $B \vDash \varphi(\overline{a})$, 则由定理 1 知 $A \vDash \bigwedge \mathrm{Res}_{\varphi}(\overline{a})$, 再由 (b) 即得 $A \vDash \varphi(\overline{a})$. 所以 $A$ 是 $T$ 的 e.c. 模型. (证毕)

**注:** 由 $\mathrm{Res}_{\varphi}$ 的定义易见, 上定理中的 (b) 又可等价地改述为: $A$ 是 $T$ 的模型, 并且对 $\mathcal{L}$ 上每一 $\exists_1$ 公式 $\varphi(\overline{x})$ 及 $A$ 中任一组元 $\overline{a}$, 若有 $A \vDash \neg\varphi(\overline{a})$, 则存在 $\mathcal{L}$ 上一 $\forall_1$ 公式 $\sigma(\overline{x})$ 能使 $A \vDash \neg\sigma(\overline{a})$ 并且

$$T \vdash \forall\overline{x}(\neg\sigma(\overline{x}) \to \neg\varphi(\overline{x})).$$

**推论** 设 $T$ 为语言 $\mathcal{L}$ 上的 $\forall_1$ 理论. 则 "所造的模型 $A$ 是 $T$ 的 e.c. 模型" 这一性质是可力迫的. (注: 对于 $\forall_2$ 理论 $T$, 上述结论也成立. 但以下无用.)

**证明** (1) 设 $\varphi(\overline{x})$ 为 $\mathcal{L}$ 上任一 $\forall_1$ 公式, $\overline{c}$ 为任一组互异见证. 我们证明下列性质 $P$ 是可力迫的. $P$: 若 $A^+ \vDash \varphi(\overline{c})$, 则存在 $\mathcal{L}$ 上的 $\exists_1$ 公式 $\psi(\overline{x})$ 能使

$$T \vdash \forall\overline{x}(\psi(\overline{x}) \to \varphi(\overline{x}))$$

并且 $A^+ \vDash \psi(\overline{c})$.

考虑博奕 $G(P)$. 设甲走出了 $T$- 条件 $p_0$. 记 $\bigwedge p_0$ 为 $\rho(\overline{c}, \overline{d})$(其中 $\overline{d}$ 列举了 $p_0$ 中 $\overline{c}$ 以外的见证). 以下分二情况:

(1.1) 若 $T \cup p_0 \vdash \varphi(\overline{c})$. 此时易见有

$$T \vdash \forall\overline{x}(\exists\overline{y}\rho(\overline{x}, \overline{y}) \to \varphi(\overline{x})),$$

因而由 $A^+(\overline{p}) \vDash p_0$(见引理 6) 即知 $P$ 成立 (视 $\exists\overline{y}\rho(\overline{x},\overline{y})$ 为 $\psi(\overline{x})$).

(1.2) 若 $T \cup p_0 \nvdash \varphi(\overline{c})$. 此时 $T \cup p_0 \cup \{\neg\varphi(\overline{c})\}$ 和谐，故由引理 12 知存在 $T$- 条件 $q \supseteq p_0$ 能使 $q \vdash \neg\varphi(\overline{c})$. 因而，乙只须走出 $p_1 = q$, 则由 $A^+(\overline{p}) \vDash p_1$ (由引理 6) 即知 $P$ 的前提为假，从而 $P$ 仍成立.

(2) 由引理 10, 乙可以迫使所造的 $A \vDash T$. 由引理 7, 乙可以迫使 $A^+$ 的每个元都能由无限多个见证指称，从而易见 $A^+$ 的每一有限长元素组 $\overline{a}$ 都能由一组互异的见证 $\overline{c}$ 指称. 再将 (1) 中的 $P$ 与定理 12 的注相对照 (注意该注中的 $\neg\varphi(\overline{x})$ 及 $\neg\sigma(\overline{x})$ 各等价于 $\forall_1$ 公式及 $\exists_1$ 公式), 并利用引理 4 及定理 12, 即知本推论成立. (证毕)

**定理 13** 设 $\overline{x} = (x_1, \cdots, x_n)$, $\varphi_i(\overline{x})$ $(i = 0, 1, 2, \cdots)$ 为语言 $\mathcal{L}$ 上的一系列 $\exists_1$ 公式，而 $p$ 为一 $T$- 条件. 如果

(a) $p$ 不力迫 $\forall\overline{x} \bigvee\limits_{i<\omega} \varphi_i(\overline{x})$. 则有

(b) 存在 $\mathcal{L}(W)$ 上的无量词公式 $\psi(\overline{x})$ 能使 $T \cup p \cup \{\exists\overline{x}\psi(\overline{x})\}$ 和谐并且

$$T \vdash \forall\overline{x}(\psi(\overline{x}) \to \bigwedge_{i<\omega} \neg\varphi_i(\overline{x})).$$

(注：反之由 (b) 也可得 (a), 但此事以下无用.)

**证明** (1) 先证由 (a) 能推出

(c) 存在不出现于 $p$ 中的互异见证 $\overline{c}$ 及 $T$- 条件 $q \supseteq p$ 能使 $q$ 力迫每一 $\neg\varphi_i(\overline{c})$ $(i = 0, 1, 2, \cdots)$.

假若 (c) 不成立. 任取一组不出现于 $p$ 中的互异见证 $\overline{c} = (c_1, \cdots, c_n)$. 现在证：

$$p\text{力迫} \bigvee_{i<\omega} \varphi_i(\overline{c}). \tag{1}$$

设甲走出了 $T$- 条件 $p_0 \supseteq p$, 则由 (c) 不成立可知存在 $i$ 使

$p_0$ 不力迫 $\neg\varphi_i(\bar{c})$. 故由引理 9 知乙能把 $p_0$ 扩充为一 $T$- 条件 $p_1$ 使 $p_1$ 力迫此 $\varphi_i(\bar{c})$, 因而此后乙即可迫使 $A^+(\bar{p}) \models \varphi_i(\bar{c})$, 从而有 $A^+ \models \bigvee_{i<\omega} \varphi_i(\bar{c})$.

上段说明 (1) 式成立. 再由引理 11 可知 $p$ 力迫 $\forall\bar{x} \bigvee_{i<\omega} \varphi_i(\bar{x})$, 这与 (a) 矛盾.

(2) 再证明由 (c) 可推出 (b).

对于 (c) 中的 $\bar{c}$ 及 $q$, 记 $\bigwedge q$ 为 $\psi(\bar{c})$.

由 $q$ 为 $T$- 条件知 $T \cup q$ 和谐, 从而 $T \cup q \cup p$ 和谐, 再由 $\psi(\bar{c})$ 定义知 $T \cup p \cup \psi(\bar{c})$ 及 $T \cup p \cup \{\exists\bar{x}\psi(\bar{x})\}$ 和谐.

对每个 $i$. 由 (c) 知 $q$ 力迫 $\neg\varphi_i(\bar{c})$. 后者等价于一 $\forall_1$ 语句 $\forall\bar{y}\rho_i(\bar{y},\bar{c})$ ($\rho_i$ 中无量词). 现在任取一组不出现于 $q$ 及 $\varphi_i$ 及 $\bar{c}$ 中的互异见证 $\bar{d}$, 则由以上有 $\neg\varphi_i(\bar{c}) \vdash \rho_i(\bar{d},\bar{c})$, 从而显见 $q$ 力迫 $\rho_i(\bar{d},\bar{c})$. 再由 $\rho_i(\bar{d},\bar{c})$ 为无量词语句及定理 11 可知 $T \cup q \vdash \rho_i(\bar{d},\bar{c})$, 从而有 $T \cup q \vdash \forall\bar{y}\rho_i(\bar{y},\bar{c})$ 及 $T \cup q \vdash \neg\varphi_i(\bar{c})$. 由此有 $T \vdash \psi(\bar{c}) \to \neg\varphi_i(c)$ 及 $T \vdash \forall\bar{x}(\psi(\bar{x}) \to \neg\varphi_i(\bar{x}))$.

由以上两段即知 (b) 成立. (证毕)

**定义** 语言 $\mathcal{L}$ 上的一集 $\forall_1$ 公式 $\Phi(\bar{x})$(其中 $\bar{x}$ 为一组互异的自由变元 $(x_1,\cdots,x_n)$) 称为一个 **$\forall$- 集**. 若 $\mathcal{L}$ 的模型 $A$ 中有一 $n$ 元组 $\bar{a}$ 能适合 $\Phi(\bar{x})$, 称 $\Phi(\bar{x})$ 能 **被 $A$ 实现**. 否则称 $\Phi(\bar{x})$ **被 $A$ 省略**.

**定义** 设 $\Phi(\bar{x})$ 为 $\mathcal{L}$ 上一个 $\forall$- 集, $\psi(\bar{x})$ 为 $\mathcal{L}$ 上一个 $\exists_1$ 公式, $T$ 为 $\mathcal{L}$ 上的理论. 若 $T \cup \{\exists\bar{x}\psi(\bar{x})\}$ 和谐并且对每一 $\varphi(\bar{x}) \in \Phi(\bar{x})$ 都有

$$T \vdash \forall\bar{x}(\psi(\bar{x}) \to \varphi(\bar{x}))$$

成立, 则称 $\psi(\bar{x})$ 为 $\Phi(\bar{x})$ 的一个 **支撑**.

以下在讨论群时, 仍设 $\mathcal{L}$ 及 $T$ 如引理 1 之前所述.

**定理 14** 设 $\Phi_j(\bar{x})$ ($j = 0,1,2,\cdots$; $\bar{x}$ 的长度 $n$ 固定) 均为无支撑的 $\forall$- 集. 则存在 e.c. 群能省略所有的 $\Phi_j(\bar{x})$.

**证明** (1) 先证明，对每个 $j$，都不存在 $\mathcal{L}(W)$ 上的 $\exists_1$ 公式 $\psi(\overline{x})$ 能使：$T\cup\{\exists\overline{x}\psi(\overline{x})\}$ 和谐并且对每个 $\varphi(\overline{x})\in\Phi_j(\overline{x})$ 都有

$$T\vdash\forall\overline{x}(\psi(\overline{x})\to\varphi(\overline{x})).$$

假若存在这样的 $\psi(\overline{x})$，则其形状为 $\exists\overline{y}\rho(\overline{y},\overline{x})$. ($\rho$ 中无量词)，设其中出现的 $W$ 中常量为 $c_1,\cdots,c_m$，则 $\psi(\overline{x})$ 可记为 $\exists\overline{y}\rho(\overline{y},c_1,\cdots,c_m,\overline{x})$. 现在令 $\psi_1(\overline{x})$ 为 $\exists\overline{y}\,\overline{z}\rho(\overline{y},\overline{z},\overline{x})$ ($\overline{z}=(z_1,\cdots,z_m)$)，则 $\psi_1(\overline{x})$ 为 $\mathcal{L}$ 上的公式，并且由 $\psi(\overline{x})$ 的性质易知：$T\cup\{\exists\overline{x}\psi_1(\overline{x})\}$ 和谐并且对每个 $\varphi(\overline{x})\in\Phi_j(\overline{x})$ 都有 (注意 $\varphi(\overline{x})$ 为 $\mathcal{L}$ 上的公式)

$$T\vdash\forall\overline{x}(\psi_1(\overline{x})\to\varphi(\overline{x})).$$

这表明 $\psi_1(\overline{x})$ 是 $\Phi_j(\overline{x})$ 的支撑，与题设矛盾.

(2) 对每个 $j$，把 $\Phi_j(\overline{x})$ 中诸公式 $\varphi(\overline{x})$ 的否定看作定理 13 中的诸 $\varphi_i(\overline{x})$，则由 (1) 及该定理易见：空集可力迫 "$\Phi_j(\overline{x})$ 被省略".

(3) 由 (2) 及定理 12 的推论及引理 4 即知本定理的结论成立. (证毕)

**定理 15**(Macintyre) 设 $H$ 为一有限生成的群，其字问题递归不可解. 则存在一 e.c. 群 $G$ 使 $H$ 不能嵌入 $G$ 中.

**证明** 取 $H$ 的一组 (有限个) 生成元 $\overline{h}$，令

$$\Phi(\overline{x})=\{\varphi(\overline{x})|\ \varphi(\overline{x})\ \text{为一等式或不等式，并且}\ H\vDash\varphi(\overline{h})\}.$$

以下证明 $\Phi(\overline{x})$(视为 $\forall$- 集) 无有支撑，从而由定理 14 知存在一 e.c. 群 $G$ 能省略 $\Phi(\overline{x})$，再由 $\Phi(\overline{x})$ 定义即知 $H$ 不能嵌入 $G$ 中.

假设 $\Phi(\overline{x})$ 有一支撑 $\psi(\overline{x})$.

(1) 现在证明，对 $\mathcal{L}$ 上任一等式 $\varphi(\overline{x})$：$\varphi(\overline{x})\in\Phi(\overline{x})$ 当且只当 $T\vdash\forall\overline{x}(\psi(\overline{x})\to\varphi(\overline{x}))$.

(1.1) 由支撑的定义可知，若 $\varphi(\overline{x})\in\Phi(\overline{x})$，则

$$T\vdash\forall\overline{x}(\psi(\overline{x})\to\varphi(\overline{x})).$$

(1.2) 若某等式 $\varphi(\overline{x}) \notin \Phi(\overline{x})$, 则由 $\Phi(\overline{x})$ 定义知 $\neg\varphi(\overline{x}) \in \Phi(\overline{x})$, 再仿 (1.1) 有 $T \vdash \forall\overline{x}(\psi(\overline{x}) \to \neg\varphi(\overline{x}))$, 从而易见 (注意由支撑定义知 $T \cup \{\exists\overline{x}\psi(\overline{x})\}$ 和谐)

$$T \nvdash \forall\overline{x}(\psi(\overline{x}) \to \varphi(\overline{x})).$$

(2) 由 (1) 可知: 在 $H$ 中成立的等式 $\varphi(\overline{h})$ 所成之集为递归可枚举.

(3) 仿 (1) 可证, 对 $\mathcal{L}$ 上任一等式 $\varphi(\overline{x})$ : $\varphi(\overline{x}) \notin \Phi(\overline{x})$ 当且只当 $T \vdash \forall\overline{x}(\psi(\overline{x}) \to \neg\varphi(\overline{x}))$. 从而可知: 在 $H$ 中不成立的等式 $\varphi(\overline{h})$ 所成的集也为递归可枚举. 再由 (2) 即易见 $H$ 的字问题为递归可解. 这与题设矛盾. (证毕)

**定理 16** 设 $H_i$ $(i = 0, 1, 2, \cdots)$ 是可数多个群, 都能由 $n$ 个生成元生成 ($n$ 不随 $i$ 而变), 并且其字问题都递归不可解. 则存在一 e.c. 群 $G$ 使每个 $H_i$ 都不能嵌入 $G$ 中.

证法与定理 15 者类似, 略去.

**定理 17** 设 $H$ 为一有限生成的群. 则 $H$ 的字问题递归可解当且只当 $H$ 能嵌入每一 e.c. 群中.

**证明** 由定理 9 及定理 15 即见.

**定理 18** 对每一递归可枚举的 Turing 度 $d$, 都存在一个有限给出的群 $G$, 其字问题的不可解度为 $d$.

证明可参看 [8].

**定理 19** 对每个可数的偏序集 $\Pi$, 都存在一集递归可枚举度, 这些度按 Turing 归约性所构成的偏序集与 $\Pi$ 同构.

证明可参看专著 [9]§ 4 的推论 3 者.

**定理 20** 存在自然数集 $\omega$ 的 $2^\omega$ 个无限子集 $X_\alpha$ $(\alpha < 2^\omega)$ 能使: 对任二不同的足码 $\alpha_1, \alpha_2$, 差集 $X_{\alpha_1} \setminus X_{\alpha_2}$ 都不空.

证明可参看专著 [10]p.48 定理 1.3 者.

下面是本章的主要定理. (其中 $\mathcal{L}$ 仍为 $\{\cdot, ^{-1}, 1\}$.)

**定理 A** 存在 $2^\omega$(连续统的基数) 个可数的存在封闭群 $G_\alpha$ ($\alpha < 2^\omega$) 适合：对任二不同的足码 $\alpha_1, \alpha_2$, 都存在一 $\mathcal{L}$ 上的 $\exists_3$ 语句 $\varphi_{\alpha_1\alpha_2}$ 能使 $G_{\alpha_1} \models \varphi_{\alpha_1\alpha_2}$ 而 $G_{\alpha_2} \models \neg\varphi_{\alpha_1\alpha_2}$.

**证明** (1) 设 $\Pi$ 为一由可数无限多生成元生成的自由格. 由定理 19 知存在一集递归可枚举的不可解度，这些度按 Turing 可归约的偏序构成与 $\Pi$ 同构的格. 在一任意取定的同构对应下，令 $d_i$ ($i < \omega$) 为与 $\Pi$ 的诸生成元对应的度，并对每个 $i < \omega$, 令 $H_i$ 为一个字问题不可解度为 $d_i$ 的有限给出的群 (由定理 18 知 $H_i$ 存在).

取 $\omega$ 的 $2^\omega$ 个无限子集 $X_\alpha$ ($\alpha < 2^\omega$) 使适合：若 $\alpha_1 \neq \alpha_2$, 则 $X_{\alpha_1} \setminus X_{\alpha_2}$ 不空. (由定理 20 知这些 $X_\alpha$ 存在.) 对每一 $\alpha < 2^\omega$, 令 $K_\alpha$ 为诸 $H_i$ ($i \in X_\alpha$) 的直和.

对每个 $\alpha < 2^\omega$, 令 $T_\alpha = T \cup \mathrm{diag}(K_\alpha)$, 以下要用 $T_\alpha$- 力迫法构造一个 e.c. 群 $G_\alpha \supseteq K_\alpha$. 我们断言，性质："对每一自然数 $j \notin X_\alpha$, $H_j$ 都不能嵌入 $G_\alpha$ 中" 是可力迫的.

(2) 现在证明上述的断言.

设 $j \notin X_\alpha$, 令 $\bar{h}$ 为 $H_j$ 的一组生成元，令

$$\Phi(\bar{x}) = \{\varphi(\bar{x}) \mid \varphi(\bar{x}) \text{ 为等式或不等式，并且 } H_j \models \varphi(\bar{h})\}.$$

我们证明 $\Phi(\bar{x})$ 没有支撑，从而由定理 13 即知性质 "$\Phi(\bar{x})$ 被省略" 是可力迫的.

假若 $\Phi(\bar{x})$ 有一支撑 $\psi(\bar{x})$, 则 $T_\alpha \cup \{\exists\bar{x}\psi(\bar{x})\}$ 和谐并且

(a) $T_\alpha \vdash \forall\bar{x}(\psi(\bar{x}) \to \bigwedge\Phi(\bar{x}))$.

$\psi(\bar{x})$ 是 $T_\alpha$ 的语言上的公式，其中可以出现有限多个指称 $K_\alpha$ 中元素的新常量. 现在把 $K_\alpha$ 改写为 $K'_\alpha \times K''_\alpha$, 使 $K'_\alpha$ 是有限个 $H_i$ ($i \in X_\alpha$) 的直和并且 $\psi(\bar{x})$ 中新常量所指称的元素都在 $K'_\alpha$ 中. 现在证明

(b) $T \cup \mathrm{diag}(K'_\alpha) \vdash \forall\bar{x}(\psi(\bar{x}) \to \bigwedge\Phi(\bar{x}))$.

这是因为：否则将存在 $T \cup \mathrm{diag}(K'_\alpha)$ 的模型 $A$, 它含有一组元 $\bar{a}$ 使

$A \models \psi(\bar{a})$ 并且对某个 $\varphi(\bar{x}) \in \Phi(\bar{x})$ 有 $A \models \neg\varphi(\bar{a})$. 考虑群 $A \times K''_\alpha$, 易见 $K_\alpha \subseteq A \times K''_\alpha$, 从而 $A \times K''_\alpha \models T_\alpha$. 又因 $\psi(\bar{x})$ 及 $\neg\varphi(\bar{x})$ 都是 $\exists_1$ 公式而 $A$ 为 $A \times K''_\alpha$ 的子群, 故由以上有 $A \times K''_\alpha \models \psi(\bar{a}) \wedge \neg\varphi(\bar{a})$. 易见这与 (a) 矛盾, 所以 (b) 成立.

设 $K'_\alpha = H_{i_1} \times \cdots \times H_{i_k}$ $(i_1, \cdots, i_k \in X_\alpha)$. 如果我们会解 $H_{i_1}$ 及 $H_{i_2}$ 及 $\cdots$ 及 $H_{i_k}$ 的字问题, 则易见也就会解 $K'_\alpha$ 的字问题. 从而再由 $(\bar{b})$ 及 $\Phi(\bar{x})$ 的定义可知也就会解 $H_j$ 的字问题 (其理由可参看定理 15 的证法). 再根据 Church 论题及诸 $H_i$ 的取法, 就可知应有

$$d_j \leqslant d_{i_1} \vee d_{i_2} \vee \cdots \vee d_{i_k}.$$

但由 $j \notin X_\alpha$ 及 $\Pi$ 为自由格又知

$$d_j \not\leqslant d_{i_1} \vee d_{i_2} \vee \cdots \vee d_{i_k}.$$

这就得到矛盾. 所以 $\Phi(\bar{x})$ 没有支撑.

(3) 对每个 $\alpha < 2^\omega$, 由 (2) 及 $T_\alpha$- 力迫法诸性质及引理 4 即知: 存在一个可数的 e.c. 群 $G_\alpha$, 它适合 $T_\alpha$(从而 $K_\alpha$ 可嵌入其中, 再由 $K_\alpha$ 定义即知每个 $H_i$ 之 $i \in X_\alpha$ 者均可嵌入 $G_\alpha$ 中), 并且对每个 $j \notin X_\alpha$, 相应的 $\Phi(\bar{x})$ 被 $G_\alpha$ 省略 (由 $\Phi(\bar{x})$ 定义可知这就是说 $H_j$ 不能嵌入 $G_\alpha$ 中).

(4) 若 $\alpha_1 \neq \alpha_2$ $(\alpha_1, \alpha_2 < 2^\omega)$, 任取 $i \in X_{\alpha_1} \setminus X_{\alpha_2}$, 则由 (3) 可知 $H_i$ 能嵌入 $G_{\alpha_1}$ 而不能嵌入 $G_{\alpha_2}$ 中. 再由定理 9 的推论即知: 存在 $\mathcal{L} = \{\cdot, ^{-1}, 1\}$ 上的 $\exists_3$ 语句 $\sigma_{H_i}$ 能使 $G_{\alpha_1} \models \sigma_{H_i}$ 而 $G_{\alpha_2} \models \neg\sigma_{H_i}$, 取 $\sigma_{H_i}$ 作为 $\varphi_{\alpha_1\alpha_2}$ 即可. (证毕)

关于 e.c. 群, 用模型论方法还可证明不少进一步的结果. 举例如下 (证明略去):

**定理 B** 存在 $2^\omega$ 个互不同构的可数的存在封闭群 $G_\alpha$ $(\alpha < 2^\omega)$ 适合:

(a) 这些 $G_\alpha$ 都初等等价. (即: 它们所适合的 $\mathcal{L} = \{\cdot, ^{-1}, 1\}$ 上的 1 阶语句完全相同.)

(b) 若 $H$ 为一有限生成的群且能同构嵌入两个 $G_{\alpha_1}, G_{\alpha_2}$ ($\alpha_1 \neq \alpha_2$) 中, 则 $H$ 的字问题递归可解.

证明见 [3] 中定理 4.1.6 者.

**定理 C** 存在 $2^\omega$ 个可数的存在封闭的 2 类幂零群 $G_\alpha$ ($\alpha < 2^\omega$) 适合: 若 $\alpha_1 \neq \alpha_2$, 则 $G_{\alpha_1}$ 不能同构嵌入 $G_{\alpha_2}$ 中.

(注: 2 类幂零群 $G$ 的一种定义是: 对任何 $a, b \in G$, 其换位元 $[a, b]$ 都被包含在 $G$ 的中心内.)

证明见 [3] 中定理 4.4.5 者.

**定理 D** 只存在 1 个周期的 (即: 元素周期都有限的) 可数的存在封闭 2 类幂零群.

证明见 [3] 中定理 4.4.6 者.

## 参考文献


1 Scott R W. Algebraically closed groups. Proc. Amer. Math. Soc., 1951, 2: 118～121

2 Higman G, Scott E. Existentially Closed Groups. Oxford: Clarendon Press, 1988

3 Hodges W. Building Models by Games. Cambridge: Cambridge University Press, 1985

4 王世强. 模型论基础. 北京: 科学出版社, 1987

5 Lyndon R, Schupp P. Combinatorial Group Theory. Heidelberg: Springer–Verlag, 1977

6 Neumann B H, Neumann H. Embedding theorems for groups. Jour. London Math. Soc., 1959, 34: 465～479

7 Rotman J. The Theory of Groups (2nd edition). Boston: Allyn and Bacon Inc., 1973

8 Clapham C. Finitely presented groups with word problems of arbitrary degrees of insolubility. Proc. London Math. Soc., 1964, 14: 633~676

9 Sacks G. Degrees of Unsolvability. Princeton: Princeton University Press, 1963

10 Kunen K. Set Theory. Amsterdam: North–Holland Publ. Co., 1980

# 第 8 章

# 关于 Mordell–Lang 猜想

在代数几何中， S. Lang 曾于 1965 年以来多次提出猜想，以推广 L. J. Mordell 在 1922 年提出的猜想“亏数 $\geqslant 2$ 的有理代数曲线上有理点个数有限”及其他有关猜想. Lang 猜想的一种形式是说：“设 $K$ 为一特征数 0 的域， $S$ 是 $K$ 上的一个半 Abel 簇， $X$ 是 $S$ 的一个闭子簇. 设 $\Gamma$ 是 $S$ 的一个有限秩的子群 (即：张量积 $\Gamma \otimes \mathbf{Q}$ 在有理数域 $\mathbf{Q}$ 上维数有限). 此时，存在 $S$ 的有限个代数子群的陪集 $B_1, \cdots, B_m$ 能使 $X \cap \Gamma \subseteq B_1 \cup \cdots \cup B_m$.” 后来，又有人对特征数 $p > 0$ 的情况研究类似的问题，通称 Mordell–Lang 猜想. (它的一种关于函数域 $K$ 的一般形式见以下定理 H 及其推论.)

对于 $K$ 为数域的情况，这一猜想已被 G. Faltings 等人证明. 对于函数域的情况，在下述文献 [1] 的工作之前，人们只解决了一部分情况，并且所用的方法各不相同. 在 1996 年发表的 [1] 中，E. Hrushovski 在模型论中稳定性理论已有成果的基础上，结合模型论方法与代数几何方法，对 $K$ 为函数域的情况 (特征数任意) 给出了一个完整而统一的证明. 这一结果受到有关专家们的广泛注意.

由于 Hrushovski 的证明用到了模型论中不少概念和结果，所

以不能在此详细介绍. 以下只简单介绍其证明的一个梗概. (实际只是略述建立在众多概念及预备结果基础上的最后几步论证.) 从中可以大致看出其证明途径与一般的代数几何方法不同.

## §1 Hrushovski 定理简介

设 $k$ 为一代数闭域, $K$ 为 $k$ 的一个扩域.

以 $p$ 记 $k$ 的特征数, 令

$$\text{域 } Q_p = \begin{cases} \text{有理数域 } \mathbf{Q}. \ (\text{当 } p = 0 \text{ 时}) \\ \left\{\dfrac{m}{n} \in \mathbf{Q} \mid n \text{ 与 } p \text{ 互素}\right\}. \ (\text{当 } p > 0 \text{ 时}) \end{cases}$$

称一个群 $\Gamma$ 为 $p'$- 有限生成的, 如果 $\Gamma \otimes Q_p$ 作为 $Q_p$- 模是有限生成的.

称一个 Abel 簇用一个代数环面 (torus) 的扩张为半 Abel 簇.

在上述记号下, Hrushovski 的主要结果是:

**定理 H** 设 $S$ 是一个定义在 $K$ 上的半 Abel 簇, $X$ 是 $S$ 的一个子簇. 设 $\Gamma$ 是 $S$ 的一个 $p'$- 有限生成的子群, 并设 $X \cap \Gamma$ 在 $X$ 中是 Zariski 稠密的. 此时, 存在一个定义在 $k$ 上的半 Abel 簇 $S_0$, 及 $S_0$ 的一个定义在 $k$ 上的子簇 $X_0$, 以及由 $S$ 的一个群子簇到 $S_0$ 中的一个有理同态 $h$, 能使 $X$ 成为 $h^{-1}(X_0)$ 的一个迁移 (即成为 $h^{-1}(X_0) + c$ 形状).

如果我们把 $S$ 的适合下列条件的子簇 $X$ 暂称为特殊的, 即: "存在 $S$ 的一个群子簇 $S_1$, 一个定义在 $k$ 上的半 Abel 簇 $S_0$, 及 $S_0$ 的一个定义在 $k$ 上的子簇 $X_0$, 以及一个有理同态 $h$: $S_1 \longrightarrow S_0$ 能使 $X$ 成为 $h^{-1}(X_0)$ 的一个迁移". 则由定理 H 可得下列的

**推论** 设 $S$ 及 $\Gamma$ 如定理 H 所述. 此时, 对于 $S$ 的任何子簇 $Z$, $Z \cap \Gamma$ 都能被包括在 $S$ 的有限个特殊子簇的并集之中.

**证明** 只需把定理 H 应用于 $Z\cap\Gamma$ 的 Zariski 闭包的诸不可约部分上即可.

为了简介定理 H 的证明大意, 我们先列出一些引理. 关于这些引理的证明及其中所涉及概念的定义 (有不少是模型论概念), 可参看文献 [1],[2] 及 [3].

**引理 1** 设 $G$ 为一 Morley 维数有限的可换群, $A\neq\{0\}$ 为 $G$ 的一个可 1 阶定义的连通子群, $X$ 为 $G$ 的一个可 $(\infty)1$ 阶定义的重数为 1 的子集. 又设:

(i) $A$ 为 $(G/A)$- 刚性 (rigid) 的.

(ii) 不存在 $G$ 的可 1 阶定义的子群 $A'\supset A$ 能使: $A'/A$ 为无限, 并且对某个极小的 $Y$ 及有限的 $C$ 有 $A'\subseteq \mathrm{acl}(Y,A,C)$.

(iii) $\mathrm{Stab}(X)\cap A$ 为有限集.

此时, $X$ 除了一个维数较小的子集之外, 能被包括在 $A$ 的单一个陪集之中.

证明见 [1] 的引理 4.3.

**引理 2** 设可换群 $A=A_1+A_2$, 其中 $A_1,A_2$ 为互相正交的半极小子群, 并且 $A_1$ 是线性型的. 令 $X\subseteq A$ 为 $\mathrm{acl}(\phi)$ 上一个完备型的解集合. 如果 $\mathrm{Stab}(X)$ 为有限集, 则 $X$ 被包括在 $A_2$ 的一个陪集中.

证明见 [1] 的引理 4.15.

在下列的引理 3 至引理 5 及定理 1 中, $K$ 及 $k$ 为如下的域: 对于特征数 $p>0$, $K$ 为一可分闭域, 具有一个取定的有限 $p$- 基底, 并且 $K$ 是饱和的; $k=\cap_n K^{p^n}$ (易知 $k$ 为代数闭域). 对于特征数 $p=0$, $K$ 为一微分闭域, 并且 $K$ 是饱和的; $k$ 为 $K$ 的常数域 $\{x\in K\mid Dx=0\}$ (易知 $k$ 为代数闭域).

**引理 3** 设 $X$ 为一 Zariski 极小型, 则: 或者 $X$ 为局部模度 (modular) 的, 或者 $X$ 不正交于 $k$.

证明见 [1] 的引理 5.4.

**引理 4** 设 $G$ 为一个定义在 $K$ 上的半 Abel 簇，$A$ 为 $G$ 的一个半极小的可 1 阶定义的子群，它在 $G$ 中为 Zariski 稠密. 此时：或者 $A$ 为局部模度的；或者存在一个定义在 $k$ 上的代数群 $H$ 及一个 1-1 到上的有理同态映射 $h: G \to H$ 能使 $h(A) = H(k)$.

证明见 [1] 的引理 5.6.

**引理 5** 设 $G$ 为一个定义在 $K$ 上的半 Abel 簇，$A$ 为 $G$ 的一个半多重极小 (pluriminimal) 的可 1 阶定义的子群. 则 $A$ 为 (强) 刚性的.

证明见 [1] 的引理 5.7.

**定理 1** 设 $K$ 是如上所述的饱和域. 设 $S$ 是一个定义在 $K$ 上的半 Abel 簇，$X$ 是 $S$ 的一个子簇. 设 $\Gamma$ 是 $S$ 的一个可 $\infty$ 1 阶定义的子群，其维数有限，并设 $X \cap \Gamma$ 在 $X$ 中为 Zariski 稠密. 此时，存在一个定义在 $k$ 上的半 Abel 簇 $S_0$，及 $S_0$ 的一个定义在 $k$ 上的子簇 $X_0$，以及由 $S$ 的一个群子簇到 $S_0$ 中的一个有理同态映射 $h$，能使 $X$ 成为 $h^{-1}(X_0)$ 的一个迁移.

**证明大意** 我们不妨设 $X$ 的稳定子为有限集 (否则可通过作商集去掉它的连通部分). 令 $A$ 为 $\Gamma$ 的极大半多重极小连通子群. 此时，引理 1 的 (ii) 成立. 又由引理 5 知，引理 1 的 (i) 也成立.

由题设，$X \cap \Gamma$ 在 $X$ 中为 Zariski 稠密. 现在取一个可 1 阶定义的 $Y \subseteq X \cap \Gamma$ 使 $Y$ 在 $X$ 中为 Zariski 稠密，并且 $Y$ 有最小可能的维数和重数. 由于 $X$ 不可约，每当 $Y$ 被表为一个有限并 $\cup_i Y_i$ 时，其中必有一 $Y_i$ 在 $X$ 中为 Zariski 稠密. 所以 $Y$ 的重数为 1. 另外，若 $Y'$ 是 $Y$ 的一个维数相同的子集，则 $Y'$ 也是在 $X$ 中 Zariski 稠密的，因为其余集 $Y \setminus Y'$ 不能在 $X$ 中 Zariski 稠密.

如果 $A$ 中一元 $a$ 对 $Y$ 的迁移能够在下述意义下使 $Y$ 稳定，即：$\dim(Y \cap (Y+a)) = \dim(Y)$，则 $Y \cap (Y+a)$ 的 Zariski 闭包必为 $X$. 从而，由于 $X \cap (X+a)$ 为 Zariski 封闭且包括 $Y \cap (Y+a)$，此元 $a$ 使集合 $X$ 稳定. 由此可知，$Y$ 在维数意义下的稳定子被

包括在 $X$ 的集合意义下的稳定子之内，因而它是有限集.

由上可知，引理 1 的 (iii) 对 $Y$ 成立.

故由引理 1 可知，$Y$ 有一个维数相同的子集 $Y'$ 能被包括在 $A$ 的单一个陪集 $A+c$ 中. 特知 $(A+c)\cap X$ 在 $X$ 中为 Zariski 稠密.

现在，把 $X$ 用 $X-c$ 替换，并把 $\Gamma$ 用 $A$ 替换来继续讨论.

把 $A$ 表为若干正交子群 $A_i$ 的和，其中每个 $A_i$ 均为半极小的. 令 $B$ 为一切非局部模度的 $A_i$ 之和，$C$ 为其他诸 $A_i$ 之和. 假若 $A_{i_1}, A_{i_2}$ $(i_1 \neq i_2)$ 均为非局部模度的，则由引理 3 知它们都不正交于 $k$, 因而彼此也不正交，这与 $A_{i_1}, A_{i_2}$ 的取法不合. 由此知 $B$ 只由 1 个 $A_i$ 组成，因而 $B$ 为半极小的. 再由引理 2 可知，$Y$ 被包括在 $B$ 的单一个陪集中. 经过迁移，不妨设 $Y$ 被包括在 $B$ 中.

令 $G$ 为 $B$ 的 Zariski 闭包，则 $G$ 是 $S$ 的一个群子簇，并且 $X \subseteq G$(因 $X$ 是 $Y$ 的 Zariski 闭包). 由引理 4 可知, 存在一个 $k$ 上的代数群 $S_0$ 及一个定义在 $K$ 上的 1-1 到上的有理同态 $h$: $G \to S_0$ 能使 $h(B) = S_0(k)$. 所以 $S_0$ 是半 Abel 的.

令 $X_0$ 为 $h(Y)$ 的 Zariski 闭包. 由于 $h(Y) \subseteq h(B)$, $X_0$ 是在 $k$ 上可定义的.

显然 $h^{-1}(X_0)$ 包括 $X$. 又由于 $h$ 是 1-1 到上的，所以 $X = h^{-1}(X_0)$. (证毕)

由定理 1 再经过一些讨论，可以对 $K$ 去掉饱和性条件而得下列的定理 2, 但其中以 $K^*$ 记 $K$ 的一个饱和初等扩域.

**定理 2** 设 $K$ 及 $k$ 为如下的域：对于特征数 $p>0$, $K$ 为一可分闭域, 具有一个取定的有限 $p$- 基底, 并且 $k=\cap_n K^{p^n}$. 对于特征数 $p=0$, $K$ 为一微分闭域, 而 $k=\{x\in K|Dx=0\}$. 设 $S$ 为一个定义在 $K$ 上的半 Abel 簇，$X$ 是 $S$ 的一个子簇. 设 $\Gamma_n(n=1,2,3,\cdots)$ 是 $S$ 的一系列递降的在 $K$ 上可 1 阶定义的子群，能使 $\cap_n\Gamma_n(K^*)$ 在 $K^*$ 上维数有限；并且对每个 $n$, 存在 $\Gamma_n$ 的一个陪集 $C_n$ 能使

$X \cap C_n$ 在 $X$ 中为 (对于 $K^*$ 而言)Zariski 稠密. 此时, 存在一个定义在 $k$ 上的半 Abel 簇 $S_0$, 及 $S_0$ 的一个定义在 $k$ 上的子簇 $X_0$, 以及由 $S$ 的一个群子簇到 $S_0$ 中的一个有理同态映射 $h$, 能使 $X$ 成为 $h^{-1}(X_0)$ 的一个迁移.

证明见 [1] 的定理 5.9.

现在由定理 2 来证明定理 H. 为此, 再列出一条引理.

**引理 6** 设 $S$ 是一个定义在 $K^*$ 上的半 Abel 簇, 并设 $\Gamma$ 是 $S$ 的一个 $p'$- 有限生成的子群. 此时, 存在 $S$ 的一个有限维子群 $\Gamma^\circ$ 能包括 $\Gamma$.

证明见 [1] 的引理 3.1.

**定理 H 的证明大意** (I) 令 $S, X, k, \Gamma$ 如定理 H 所述. 取 $k$ 的一个有限生成的扩域 $L$, 使得 $S, X$ 及 $\Gamma$ 的一组 $p'$- 生成元能在 $L$ 上定义. (注意由 $\Gamma$ 为 $p'$- 有限生成可知 $L$ 存在.)

(II) 现在给出适合定理 2 题设的 $K$.

(2.1) 当 $k$ 的特征数 $p > 0$ 时. 易见 $[L : L^p]$ 有限并且 $\cap_n L^{p^n} = k$. 对于 $L$ 的可分闭包 $K$ 而言, 也有同样的性质成立. 所以, 此种 $K$ 就能适合定理 2 的题设.

(2.2) 当 $k$ 的特征数 $p = 0$ 时. 对 $L$ 赋予一个 $k$ 上的微分结构, 使 $k$ 成为常数域. 再取 $K$ 为 $L$ 的一个微分闭包, 则此种 $K$ 就适合定理 2 的题设.

(III) 为了适合定理 2 的题设, 以下再用 $S$ 的某种可 1 阶定义的子群来代替 $\Gamma$.

(3.1) 当 $p > 0$ 时. 令 $\Gamma_n = p^n S(K)$. 由 [1]§ 2 可知 $\cap_n \Gamma_n$ 为有限维. 对每个 $n$, 由 $\Gamma$ 为 $S(K)$ 的 $p'$- 有限生成子群可知商群 $(\Gamma/p^n\Gamma)$ 为有限, 故易见 $\Gamma$ 只与 $\Gamma_n$ 的有限个陪集相交. 从而再由题设的 $X \cap \Gamma$ 在 $\Gamma$ 中为 Zariski 稠密可知, $\Gamma_n$ 至少有一个陪集 $C_n$ 能使 $X \cap C_n$ 在 $X$ 中为 Zariski 稠密. 所以这些 $\Gamma_n$ 就能适合定理 2 的题设.

(3.2) 当 $p=0$ 时. 取一个如引理 6 中所说的 $\Gamma^{\circ}$ 充当定理 2 中的诸 $\Gamma_n$ 即可.

(IV) 由以上可知, 定理 2 的题设都已成立, 从而其结论成立. 而这也就是定理 H 的结论. (证毕)

## 参考文献


1 Hrushovski E. The Mordell-Lang conjective for function fields. Jour. Amer. Math. Soc., 1996, 9: 667~690

2 Hrushovski E, Zil'ber B. Zariski geometries. Jour. Amer. Math. Soc., 1996, 9: 1~56

3 Nesin A, Pillay A. The Model Theory of Groups. Notre Dame: Univ. Notre Dame Press, 1989

# 第 9 章

# 格值逻辑概述

## §1 格值逻辑

在多值逻辑中，命题或谓词的真假值可以是一个具有补运算 $'$ 的完备格 $L$ 中的元素. 在我们所讨论的形式语言中，出现的逻辑符号只限于命题连接词 $\wedge, \vee, \neg$ 及量词 $\exists, \forall$. 在讨论赋值时，它们分别被解释为 $L$ 中的运算 $\cap, \cup, '$ 及 sup (最小上界), inf(最大下界). 对于 $L$ 中的补运算，我们一般只要求它适合 $O' = I$ 及 $I' = O$ ($O, I$ 分别是 $L$ 的最小元，最大元). 这比一般的可补格条件要宽. 有时还需对 $L$ 附加一些条件，将随所讨论的问题而提出.

我们称这样的逻辑为格值逻辑. 它是通常 2 值逻辑的推广，具有很大的概括性. 现在举例如下：

例 1(有限布尔值逻辑). 通常的 2 值逻辑，其真假值集 $\{f, t\}$ 可以看作 2 元布尔代数. 这是最常见的有限布尔值逻辑. 一般，对于任一有限布尔代数 $B$, 设其元数为 $2^n$, 都可有一种相应的 $B$ 值逻辑，它是一种有 $2^n$ 个真假值的逻辑. 现在以 $n = 3$ 为例说明如下：

设 $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3$ 是某一形式语言 $\mathcal{L}$ 的 3 个模型. 对于 $\mathcal{L}$ 上的任

一语句 $\varphi$, 一般说来，它相对于 $\mathcal{U}_1,\mathcal{U}_2,\mathcal{U}_3$ 可能有下列 8 种真假情况：

(i) $\varphi$ 在 $\mathcal{U}_1,\mathcal{U}_2,\mathcal{U}_3$ 中都真．这时，我们简称“$\varphi$ 的真假值为 111”．

(ii) $\varphi$ 在 $\mathcal{U}_1,\mathcal{U}_2$ 中真而在 $\mathcal{U}_3$ 中假．这时简称 $\varphi$ 的真假值为 110.

……

(viii) $\varphi$ 在 $\mathcal{U}_1,\mathcal{U}_2,\mathcal{U}_3$ 中都假．这时简称 $\varphi$ 的真假值为 000.

由 $\varphi$ 的真假值，可以决定 $\neg\varphi$(非 $\varphi$) 的真假值．例如当 $\varphi$ 值为 101 时，$\neg\varphi$ 的值为 010, 我们记作 $(101)' = 010$. 对其它值也仿此定义运算“$'$”．

由两个语句 $\varphi_1,\varphi_2$ 的真假值，可以决定 $\varphi_1\wedge\varphi_2$ ($\varphi_1$ 且 $\varphi_2$) 及 $\varphi_1\vee\varphi_2$($\varphi_1$ 或 $\varphi_2$) 的真假值．例如当 $\varphi_1,\varphi_2$ 的值各为 110 及 011 时，$\varphi_1\wedge\varphi_2$ 的值为 010, 我们记作 $110\cap 011 = 010$, $\varphi_1\vee\varphi_2$ 的值为 111, 记作 $110\cup 011 = 111$. 对其它值也仿此定义运算“$\cap$”及“$\cup$”．

易见，真假值集 $\{111,110,\cdots,001,000\}$ 对于上述三运算构成 $8(=2^3)$ 元布尔代数 $B_3$.

对于这样的布尔值逻辑，我们可以仿照 2 值逻辑的情况研究它们的命题逻辑及谓词逻辑．可以作语法的研究 (侧重形式推演)，也可以作语义的研究 (侧重模型论)．

**例 2**(无限布尔值逻辑)．对于任一无限的完备布尔代数 $B$, 也可仿照例 1 考虑 $B$ 值逻辑．例如在公理集合论中，经常应用集合论的布尔值模型来研究集合论命题的和谐性及独立性问题．它是著名的力迫方法的一种表现形式．因比较专门，不在此介绍．读者可以参看公理集合论的专书．

**例 3**(有限非布尔值逻辑)．除了布尔代数之外，对于任一具有补运算 $'$ 的有限格 $L$, 都可以仿照例 1 考虑 $L$ 值逻辑．例如，J. Lukasiewicz 及 B. Rosser 等人研究过以如下的格 $L$ 的元素为真假

值的逻辑： $L=\{1,2,\cdots,m\}$ ($m$ 为任一 $\geqslant 2$ 的正整数), 格运算为

$$a\cap b=\min(a,b);\quad a\cup b=\max(a,b);\quad a'=m+1-a.$$

又如, 我们在下节将详细讨论一种关于若干人的知识状态的逻辑. 它也是一种有限非布尔值逻辑.

**例 4**(无限非布尔值逻辑). 除了布尔代数之外, 对于任一具有补运算的无限完备格 $L$, 也都可仿照例 1 考虑以 $L$ 为值格的逻辑. 例如, 在模糊数学, 概率论以及量子力学等研究中, 都有这种类型的逻辑出现. 关于这种逻辑, 我们也不在此多谈, 因为本节所讨论的模型论内容主要适用于有限值格的情况.

## §2 知识状态逻辑

作为上一节的补充, 本节专门谈一种有关知识状态的逻辑. 从其直观来源看, 这种逻辑可能会有较多的实用前景.

我们以两人知识状态为例来说明. 一般的 $m$ 人情况与此类似.

### 2.1 被知值、值表、值格

设 $p$ 为语言 $\mathcal{L}$ 中的一个语句, 现有 $A,B$ 两人 (或两台计算机) 各自根据自己的知识 (或计算机存储的信息) 来判断 $p$ 在 $\mathcal{L}$ 的某一模型 $\mathcal{U}$ 上的真假. 则可能的情况有下列 7 种 (看作 $p$ 的 7 种 “被知值”):

(i) $A,B$ 都知其为真. 我们把此种状态记作 11. (这时也可说: $p$ 的被知值为 11.)

(ii) $A$ 知其为真而 $B$ 不知其真假. 记作 $1n$.

(iii) $A$ 不知其真假而 $B$ 知其为真. 记作 $n1$.

(iv) $A,B$ 都不知其真假. 记作 $nn$.

(v) $A$ 不知其真假而 $B$ 知其为假. 记作 $n0$.

(vi) $A$ 知其为假而 $B$ 不知其真假. 记作 $0n$.

(vii) $A, B$ 都知其为假. 记作 00.

(注意, 由于 $p$ 在 $U$ 上的真假是确定的, 故不可能有 10 或 01 两状态.)

对于语句 $\neg p$, 易见其被知值可由 $p$ 的被知值如下决定:

| p | 11 | $1n$ | $n1$ | $nn$ | $n0$ | $0n$ | 00 |
|---|---|---|---|---|---|---|---|
| $\neg p$ | 00 | $0n$ | $n0$ | $nn$ | $n1$ | $1n$ | 11 |

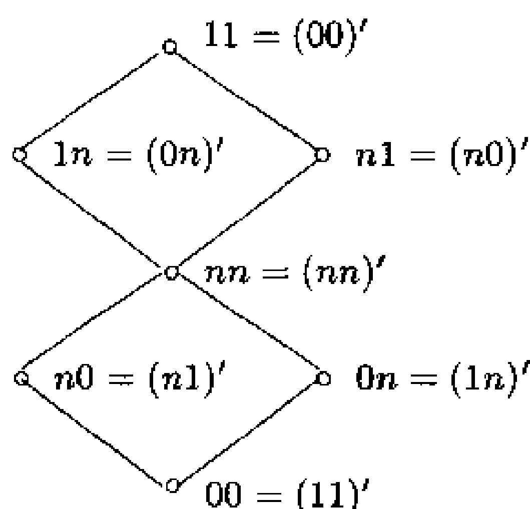
(例如: 若 $p$ 值为 $1n$, 则 $A$ 知 $p$ 真而 $B$ 不知 $p$ 的真假, 从而 $A$ 知 $\neg p$ 假而 $B$ 不知 $\neg p$ 的真假, 所以此时 $\neg p$ 的值为 $0n$.)

对于语句 $p \wedge q$ 及 $p \vee q$, 其被知值可由 $p, q$ 的被知值如下决定:

| $p \wedge q$ | 11 | $1n$ | $n1$ | $nn$ | $n0$ | $0n$ | 00 | $(q)$ |
|---|---|---|---|---|---|---|---|---|
| 11 | 11 | $1n$ | $n1$ | $nn$ | $n0$ | $0n$ | 00 | |
| $1n$ | $1n$ | $1n$ | $nn$ | $nn$ | $n0$ | $0n$ | 00 | |
| $n1$ | $n1$ | $nn$ | $n1$ | $nn$ | $n0$ | $0n$ | 00 | |
| $nn$ | $nn$ | $nn$ | $nn$ | $nn$ | $n0$ | $0n$ | 00 | |
| $n0$ | $n0$ | $n0$ | $n0$ | $n0$ | $n0$ | 00 | 00 | |
| $0n$ | $0n$ | $0n$ | $0n$ | $0n$ | 00 | $0n$ | 00 | |
| 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| $(p)$ | | | | | | | | |

| $p \vee q$ | 11 | $1n$ | $n1$ | $nn$ | $n0$ | $0n$ | 00 | $(q)$ |
|---|---|---|---|---|---|---|---|---|
| 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | |
| $1n$ | 11 | $1n$ | 11 | $1n$ | $1n$ | $1n$ | 1n | |
| $n1$ | 11 | 11 | $n1$ | $n1$ | $n1$ | $n1$ | n1 | |
| $nn$ | 11 | $1n$ | $n1$ | $nn$ | $nn$ | $nn$ | nn | |
| $n0$ | 11 | $1n$ | $n1$ | $nn$ | $n0$ | $nn$ | n0 | |
| $0n$ | 11 | $1n$ | $n1$ | $nn$ | $nn$ | $0n$ | 0n | |
| 00 | 11 | $1n$ | $n1$ | $nn$ | $n0$ | $0n$ | 00 | |
| $(p)$ | | | | | | | | |

不难看出, 被知值集 $\{11, 1n, n1, nn, n0, 0n, 00\}$ 对于由上述三表所决定的运算 ( 依次记为 $', \cap, \cup$) 构成如下的格 $K_2$:




格 $L_2$ 不是布尔代数. 但若只看运算 $\cap$ 及 $\cup$, 则 $L_2$ 可看作是由上、下两个 4 元布尔代数 $B_{上}$、$B_{下}$ 经过把 $B_{上}$ 的最小元与 $B_{下}$ 的最大元粘合 (即: 等同起来) 而成的.

注意, 上述的值表是我们对 $A, B$ 的逻辑能力的一种并不充分的反映. 例如: 当 $A$ 知道 $p$ 真时, 我们认为他从而知道 $\neg p$ 假, 也知道 $p \vee q$ 真 (不论 $q$ 如何), 等等, 这些已反映在表中. 但是, 当 $A$ 不知 $p$ 的真假时, 按照上表, $A$ 也不知道 $p \vee (\neg p)$ 的真假, 虽然 $A$ 一般是知道 $p \vee (\neg p)$ 为真的. (2.2 中还有与此相关的数学讨论.)

虽然这种反映并不充分, 但它也是有实际意义的. 因为现实世界的人们, 其知识都是不完全的. 当一个人知道一些语句为真时, 他 (在任何确定时刻) 未必能辨认由这些语句所能推出的每一条逻辑结论.

不过, 当 $\neg, \wedge, \vee$ 的值表一经确定之后, 我们对这种逻辑的数学讨论就将严格按照值表进行, 不再考虑其直观来源. 这是数学讨论所必需的. 总之, 数学讨论与其直观背景既有联系又有区别. 在讨论 $K_2$ 值逻辑的数学性质时, 不要与其直观来源相混淆.

**2.2** 恒知式.

对于上述的格 $K_2$, 可以讨论 $K_2$ 值逻辑的命题演算及谓词演

算. 我们在此只考虑命题演算.

对于命题演算中任一合式公式 $\varphi(p_1,\cdots,p_m)$, 当给定 $p_1,\cdots,p_m$ 的被知值后, 可以根据前述的值表逐步算出 $\varphi$ 的被知值. 如果无论 $p_1,\cdots,p_m$ 的被知值如何, $\varphi$ 的被知值总是 $\geqslant nn$ (即: $\varphi$ 永不能取 $n0,0n,00$ 为值). 则称 $\varphi$"恒不能被知为假", 或简称 $\varphi$ 为 ($K_2$ 值的) 恒知式.

这种恒知式, 与 2 值命题演算的恒真式是一致的. 此事的证明并不难. 由于它对考虑谓词演算的类似问题有启发, 现在附述如下 (见定理 1).

**引理 1** 设 $\varphi(p_1,\cdots,p_m)$ 为命题演算中任一合式公式. 在 $K_2$ 值逻辑中, 在对 $p_1,\cdots,p_m$ 的任一种赋值 $v_1,\cdots,v_m$ 之下:

(a) 若 $\varphi(v_1,\cdots,v_m)$ 不为 $nx$ 形 (即: $\neq n1,nn,no$), 则: 对于 $v_1,\cdots,v_m$ 中某 $v_i$ 之为 $ny$ 形者 (若有的话), 任意改为 $K_2$ 中的 $1y$ 或 $0y$ 后 (记为 $v_i^*$), 有

$$\varphi(v_1,\cdots,v_i^*,\cdots,v_m)=\varphi(v_1,\cdots,v_i,\cdots,v_m).$$

(b) 若 $\varphi(v_1,\cdots,v_m)$ 不为 $xn$ 形, 则: 对于 $v_1,\cdots,v_m$ 中某 $v_j$ 之为 $yn$ 形者 (若有的话), 任意改为 $L_2$ 中的 $y1$ 或 $y0$ 后 (记为 $v_j^*$), 有

$$\varphi(v_1,\cdots,v_j^*,\cdots,v_m)=\varphi(v_1,\cdots,v_j,\cdots,v_m).$$

**证明** 只证 (a). (b) 的证明完全类似. 我们对 $\varphi$ 的长度作归纳法.

(1) $\varphi$ 长为 1 时, 显见引理成立.

(2) 设 $\varphi$ 长 $\leqslant k$ 时引理已真. 当 $\varphi$ 长为 $k+1$ 时:

(2.1) 若 $\varphi$ 为 $(\neg\psi)$ 形状. 则:

$$\begin{aligned}\varphi(v_1,\cdots,v_i^*,\cdots,v_m)&=(\psi(v_1,\cdots,v_i^*,\cdots,v_m))'\\&=(\psi(v_1,\cdots,v_i,\cdots,v_m))'=\varphi(v_1,\cdots,v_i,\cdots,v_m).\end{aligned}$$

其中第二个等号是根据归纳假设. (注意, 由 $\varphi(v_1,\cdots,v_m)$ 不为 $nx$ 形及 $\varphi(v_1,\cdots,v_m)=(\psi(v_1,\cdots,v_m))'$ 可知 $\psi(v_1,\cdots,v_m)$ 也不为 $nx$ 形.)

(2.2) 若 $\varphi$ 为 $\psi_1\wedge\psi_2$ 形状. 由题设知 $\psi_1(v_1,\cdots,v_m)\cap\psi_2(v_1,\cdots,v_m)$ 不为 $nx$ 形, 由此及 $K_2$ 的 $\cap$ 运算表可知不外以下三种情况:

(2.2.1) $\psi_1(v_1,\cdots,v_m)$ 为 $1u$ 形且 $\psi_2(v_1,\cdots,v_m)$ 为 $1w$ 形. 此时, 由归纳假设有

$$\psi_1(v_1,\cdots,v_i^*,\cdots,v_m)=\psi_1(v_1,\cdots,v_i,\cdots,v_m)$$
$$\psi_2(v_1,\cdots,v_i^*,\cdots,v_m)=\psi_2(v_1,\cdots,v_i,\cdots,v_m),$$

从而有 $\varphi(v_1,\cdots,v_i^*,\cdots,v_m)=\varphi(v_1,\cdots,v_i,\cdots,v_m)$.

(2.2.2) $\psi_1(v_1,\cdots,v_m)$ 为 $0u$ 形. 此时, 由归纳假设有

$$\psi_1(v_1,\cdots,v_i^*,\cdots,v_m)=\psi_1(v_1,\cdots,v_i,\cdots,v_m)$$

设 $\psi_2(v_1,\cdots,v_m)=rs$. 虽然对 $\psi_2$ 未必能用归纳假设, 但由于 $v_i^*$ 与 $v_i$ 的第二分量相同, 故易见 $\psi_2(v_1,\cdots,v_i^*,\cdots,v_m)$ 的第二分量也与 $\psi_2(v_1,\cdots,v_i,\cdots,v_m)$ 的第二分量相同, 即 $\psi_2(v_1,\cdots,v_i^*,\cdots,v_m)$ 为 $ts$ 形. 从而有

$$\begin{aligned}\varphi(v_1,\cdots,v_i^*,\cdots,v_m)&=ou\cap ts=0u\cap rs\\&=\varphi(v_1,\cdots,v_i,\cdots,v_m).\end{aligned}$$

其中第二个等号由 $K_2$ 的 $\cap$ 运算表易见.

(2.2.3) $\psi_2(v_1,\cdots,v_m)$ 为 $ou$ 形. 仿 (2.2.2).

(2.3) 若 $\varphi$ 为 $\psi_1\vee\psi_2$ 形状. 可仿 (2.2) 证明.

(引理证毕)

**定理 1** 设 $\varphi(p_1,\cdots,p_m)$ 为一命题演算合式公式. 则下列二条件等价:

(a) $\varphi$ 为 $K_2$ 值恒知式.

(b) $\varphi$ 为 2 值恒真式.

**证明** (1) 由 (a) 证 (b): 假若 (b) 不成立, 则 $\varphi$ 在 2 元布尔代数 $B=\{f,t\}$ 上不恒真, 故 $\varphi$ 在 $p_1,\cdots,p_m$ 的某种取值 $v_1,\cdots,v_m$(诸 $v_i\in B$) 下得值 $f$. 现在考虑由 $B$ 到 $K_2$ 内的映射 $\rho$:

$$\rho(t)=11,\qquad \rho(f)=00.$$

易见 $\rho$ 保持运算 $\cap,\cup$ 及 $'$, 所以是一同构嵌入. 由此易知, 在 $K_2$ 值逻辑中, $\varphi$ 在 $p_1,\cdots,p_m$ 取值 $\rho(v_1),\cdots,\rho(v_m)$ 时得值 00. 此与 (a) 矛盾.

(2) 由 (b) 证 (a): 假若 (a) 不成立, 则在 $p_1,\cdots,p_m$ 的某种取值 $v_1,\cdots,v_m$ (诸 $v_i\in K_2$) 下有 $\varphi(v_1,\cdots,v_m)=n0$ 或 $0n$ 或 00.

(2.1) 若 $\varphi(v_1,\cdots,v_m)=0n$. 此时, 把 $v_1,\cdots,v_m$ 中凡为 $nx$ 形者都各自改为 $K_2$ 中的 $1x$ 或 $0x$, 得 $v_1^*,\cdots,v_m^*$, 则屡用引理 1 可得

$$\varphi(v_1^*,\cdots,v_m^*)=\varphi(v_1,\cdots,v_m)=0n.$$

在 $\varphi(v_1^*,\cdots,v_m^*)$ 的算值过程中若只注意诸值的第一分量, 并与 2 值逻辑对照, 即可知 $\varphi(p_1,\cdots,p_m)$ 不是 2 值恒真式. 此与 (b) 矛盾.

(2.2) 若 $\varphi(v_1,\cdots,v_m)=n0$ 或 00. 仿 (2.1). (证毕)

在谓词演算中, 我们有与定理 1 类似的定理, 现在只叙述如下, 其证明留给读者.

**定理 2** 设 $\mathcal{L}$ 为任一语言, $\varphi$ 为 $\mathcal{L}$ 中任一 1 阶语句. 则下列二条件等价:

(a) $\varphi$ 在 $\mathcal{L}$ 的每一 $K_2$ 值模型上的值都 $\geqslant nn$. (简称: $\varphi$ 为 $K_2$ 值恒知式)

(b) $\varphi$ 在 $\mathcal{L}$ 的每一 2 值模型上的值都是 $t$.

(注) 格值模型的定义见第 11 章.

## §3 格值逻辑应用举例

**3.1** 多值逻辑常被用于解决命题演算及谓词演算中的独立性问题. 即用来证明由某些合式公式及推演法则不可能推出某些合式公式. 格值逻辑是一类较特殊的多值逻辑, 它们也常能起到这样的作用. 现举一例如下:

**定理 3** 设 $\varphi_1, \varphi_2, \cdots, \varphi_8$ 及 $\psi_1, \psi_2, \psi_3$ 为如下的合式公式:

$\varphi_1$ : $p \to (q \to p)$. (其中 $X \to Y$ 代表 $(\neg X) \vee Y$, 以下仿此.)

$\varphi_2$ : $(p \vee p) \to p$. $\varphi_3$ : $p \to (p \vee q)$.

$\varphi_4$ : $p \to p$. $\varphi_5$ : $p \to \neg\neg p$.

$\varphi_6$ : $(p \to (q \to r)) \to ((p \to q) \to (p \to (r \vee \neg\neg r)))$.

$\varphi_7$ : $(\neg p \to \neg q) \to (q \to (p \vee \neg\neg p))$.

$\varphi_8$ : $(\forall x)(p \to R(x)) \to (p \to (\forall x)(R(x) \vee \neg\neg R(x)))$.

(其中 $R$ 为一 1 元谓词变元, 也即 1 元关系符号.)

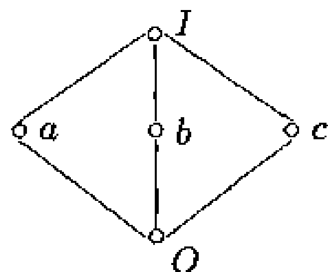
$\psi_1$ : $p \to (p \wedge \neg\neg p)$. $\psi_2$ : $(\neg\neg p) \to p$.

$\psi_3$ : $(\forall x)(p \to R(x)) \to (p \to (\forall x)R(x))$.

则: 由 $\varphi_1, \varphi_2, \cdots, \varphi_8$ 用分离法则, 推广法则 (即: 由 $A$ 推出 $(\forall \alpha)A$, 其中 $\alpha$ 为任一个体变元.) 及诸代换法则 (指: 命题变元的, 约束个体变元的, 自由个体变元的及谓词变元的代换法则) 不可能推演出 $\psi_1, \psi_2, \psi_3$.

**证明** 由于 $\varphi_1, \varphi_2, \cdots, \varphi_8$ 及 $\psi_1, \psi_2, \psi_3$ 都是 2 值恒真式, 所以, 用 2 值逻辑的值表计算难以证明定理的结论. 现在用一种格值逻辑证明如下:

令 $L$ 为右图所示的值格：其补元运算为：$I' = O$, $O' = I$, $a' = b$, $b' = c$, $c' = a$. 在 $L$ 值逻辑中，易知 $\varphi_1, \varphi_2, \cdots, \varphi_8$ 都是恒 $I$ 式 ($\varphi_8$ 的恒 $I$ 性证明见下). 并且易知分离法则，推广法则及诸代换法则都保持恒 $I$ 性.




但 $\psi_1, \psi_2, \psi_3$ 都不是恒 $I$ 式 (见下). 所以，它们都不能由 $\varphi_1, \varphi_2, \cdots, \varphi_8$ 用所说的诸法则推出.

现在证明 $\psi_1, \psi_2, \psi_3$ 的非恒 $I$ 性及 $\varphi_8$ 的恒 $I$ 性如下：

(1) 当 $p$ 取值 $a$ 时，$\psi_1$ 及 $\psi_2$ 的值各为

$$a' \cup (a \cap a'') = b \cup (a \cap c) = b \cup O = b \neq I,$$

$$(a'')' \cup a = a \cup a = a \neq I.$$

所以 $\psi_1$ 及 $\psi_2$ 都不是恒 $I$ 式.

(2) 考虑 $\psi_3$ 的如下赋值：取论域 $D = \{1, 2\}$, 令 $\rho$ 为 $D$ 上如下的 $L$ 值关系：$\rho(1) = a$, $\rho(2) = c$.

在 $\psi_3$ 中，以 $\rho$ 作为 $R$ 的解释，并令 $p$ 取值 $a$. 则：$(\forall x)(p \to R(x))$ 的值为

$$\inf\{a' \cup \rho(1), a' \cup \rho(2)\} = \inf\{b \cup a, b \cup c\} = I,$$

而 $p \to (\forall x)R(x)$ 的值为

$$a' \cup \inf\{\rho(1), \rho(2)\} = b \cup \inf\{a, c\} = b \cup O = b,$$

从而 $\psi_3$ 的值为 $I' \cup b = b \neq I$. 所以 $\psi_3$ 不是恒 $I$ 式.

(3) 在 $\varphi_8$ 的任一赋值之下：

(3.1) 若 $O \notin R(x)$ 的值集，则易见 $(\forall x)(R(x) \vee \neg\neg R(x))$ 值为 $I$, 从而易见 $\varphi_8$ 值为 $I$.

(3.2) 若 $O \in R(x)$ 的值集，则 $(\forall x)(R(x) \vee \neg\neg R(x))$ 值为 $O$. 设 $p$ 值为 $\alpha$, 则 $p \to (\forall x)(R(x) \vee \neg\neg R(x))$ 值为 $\alpha' \cup O = \alpha'$, 而

$(\forall x)(p \to R(x))$ 的值 $\beta = \inf\{\alpha' \cup O, \cdots\} \leqslant \alpha'$, 从而 $\varphi_8$ 值为 $\beta' \cup \alpha'$. 但由 $L$ 的图形及补运算定义可知，无论 $L$ 中元素 $\alpha, \beta$ 如何，只要有 $\beta \leqslant \alpha'$, 必有 $\beta' \cup \alpha' = I$. 所以 $\varphi_8$ 的值为 $I$.

综合上述两情况，即知 $\varphi_8$ 是恒 $I$ 式. (证毕)

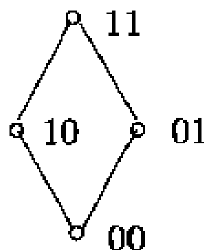
**3.2** 下面给出一个用布尔值逻辑处理代数问题的例子.

**定理 4** 设 $P$ 是一个关于群的 1 阶性质. (其确切含义为：能用下列证明所说的语言 $\mathcal{L}$ 中的语句表达的性质.) 如果对每个有限可换群 $H$ 都存在两个元数相同的扩群 $G_1$ 与 $G_2$ 能使 $G_1$ 适合 $P$ 而 $G_2$ 不适合 $P$, 则：对每个局部有限的无限可换群 $H^*$ 及每个基数 $\alpha \geqslant |H^*|$, 都存在两个基数为 $\alpha$ 的扩群 $G_1^*$ 与 $G_2^*$ 能使 $G_1^*$ 适合 $P$ 而 $G_2^*$ 不适合 $P$. ($|H^*|$ 为 $H^*$ 的基数.)

**注** 如果一个群 $G$ 的每个有限子集所生成的子群都有限，则称 $G$ 为局部有限群.

**证明** (1) 任取一个局部有限的无限可换群 $H^*$. (以下为使记号简单，对于看作模型的群 $H^*$ 和它的论域在记号上不作区分. 对其他诸群也如此.) 任取一个基数 $\alpha \geqslant |H^*|$.

令 $L$ 为如下的 4 元布尔代数，在 $L$ 值逻辑中考虑.




令语言 $\mathcal{L} = \{\rho\}$, 其中 $\rho$ 为一 3 元关系符号. 再令 $\mathcal{L}_1 = \mathcal{L} \cup \{c_h : h \text{ 通过 } H^*\}$, 其中诸 $c_h$ 为个体常量.

令 $T$ 为 $\mathcal{L}_1$ 中如下的理论 (或称分组语句集，其定义见第 11 章):

$$T = \{\varphi_1, \cdots, \varphi_5\}_{11} \cup D_{11} \cup \{\Pi\}_{10}.$$

其中诸记号说明如下.

$D$ 为 $H^*$ 的图象，即：对 $H^*$ 中每一 3 元组 $(a, b, c)$(不论 $a, b, c$ 的同异), 若在 $H^*$ 中 $a \cdot b = c$, 则把 $\rho(c_a, c_b, c_c)$ 放入 $D$ 中；若在 $H^*$

中 $a\cdot b\neq c$, 则把 $\neg\rho(c_a,c_b,c_c)$ 放入 $D$ 中. $D$ 只包含这些语句. $D_{11}$ 则表示: $D$ 中语句都放在 $T$ 的下标为 11 的组中.

诸语句 $\varphi_i$ 及 $\Pi$ 如下:

$\varphi_1$ : $(\forall xy)(\exists z)\rho(x,y,z)$.

$\varphi_2$ : $(\forall xyz_1z_2)(\rho(x,y,z_1)\wedge\rho(x,y,z_2)\to z_1\equiv z_2)$.

$\varphi_3$ : $(\forall xyzu_1u_2v_1v_2)(\rho(x,y,u_1)\wedge\rho(u_1,z,u_2)\wedge\rho(y,z,v_1)$

$\wedge\rho(x,v_1,v_2)\to u_2\equiv v_2)$.

$\varphi_4$ : $(\forall xy)(\exists z)\rho(x,z,y)$.

$\varphi_5$ : $(\forall xy)(\exists z)\rho(z,x,y)$.

$\Pi$: 在 $\mathcal{L}$ 中表达性质 $P$ 的语句.

(2) 以下将逐步证明, $T$ 具有基数为 $\alpha$ 的 $L$ 值模型 $\mathcal{U}^*$. ($L$ 值模型的定义见第 11 章.) 最后再由 $\mathcal{U}^*$ 得出定理中所说的群 $G_1^*$ 与 $G_2^*$.

任取 $T$ 的一个有限子理论 $S$. $S$ 只包含 $D$ 中有限条语句, 故由 $H^*$ 为局部有限群可知, 存在 $H^*$ 的有限子群 $H$, 能使 $S\cap D$ 被包括在 $H$ 的图象中.

对于此 $H$, 由定理题设知存在两个元数相同的扩群 $G_1$ 与 $G_2$ 能使 $G_1$ 适合 $P$ 而 $G_2$ 不适合 $P$. 设 $H$ 的元数为 $n$, $G_1$ 与 $G_2$ 的元数为 $\beta$ ($\beta$ 可为有限或无限).

现在根据 $H$ 及 $G_1$,$G_2$ 构作一个 $L$ 值模型 $\mathcal{U}_S$ 如下:

令 $\mathcal{U}_S$ 的论域 $A_S=\{1,2,\cdots,n,n+1,\cdots,\beta\}$. (若 $\beta$ 为无限基数, 则 $A_S$ 由序数 $\beta+1$ 以前的一切非 0 序数组成.) 令 $\lambda$ 为由 $A_S$ 的子集 $\{1,2,\cdots\}$ 到 $H$ 上的任一 1–1 映射, 并令 $\lambda_1\supset\lambda$ 及 $\lambda_2\supset\lambda$ 各为由 $A_S$ 到 $G_1$ 及 $G_2$ 上的任二 1–1 映射.

在 $A_S$ 上定义一个 $L$ 值 3 元关系 $r$ 作为 $\rho$ 的解释, 其定义如

下：对于 $a,b,c\in A_S$，令

$$r(a,b,c)=\begin{cases}11, & 若\ \lambda_1(a)\cdot\lambda_1(b)=\lambda_1(c)且\lambda_2(a)\cdot\lambda_2(b)=\lambda_2(c);\\ 10, & 若\ \lambda_1(a)\cdot\lambda_1(b)=\lambda_1(c)而\lambda_2(a)\cdot\lambda_2(b)\neq\lambda_2(c);\\ 01, & 若\ \lambda_1(a)\cdot\lambda_1(b)\neq\lambda_1(c)而\lambda_2(a)\cdot\lambda_2(b)=\lambda_2(c);\\ 00, & 若\ \lambda_1(a)\cdot\lambda_1(b)\neq\lambda_1(c)且\lambda_2(a)\cdot\lambda_2(b)\neq\lambda_2(c).\end{cases}$$

对于出现在 $S$ 中的诸 $c_h$，其在 $\mathcal{U}_S$ 中的解释如下：易见在 $\{1,2,\cdots,n\}$ 中存在唯一的 $i$ 能适合 $\lambda(i)=h(\in H)$，即以 $i$ 作为 $c_h$ 的解释.

$\mathcal{U}_S$ 的定义至此完成.

(3) 现在证明 $\mathcal{U}_S$ 是 $S$ 的模型．任取 $S$ 中的语句 $\pi$.

(3.1) 若 $\pi$ 为 $\varphi_1$. 现在计算它在 $\mathcal{U}_S$ 上的值如下．对任何 $a,b\in A_S$，由 $r$ 的定义易见，存在 $c_1\in A_S$ 能使 $r(a,b,c_1)=11$ 或 10，也存在 $c_2\in A_S$ 能使 $r(a,b,c_2)=11$ 或 01．所以 $(\exists z)\rho(a,b,z)$ 在 $\mathcal{U}_S$ 上值为 $\sup\{1x,y1,\cdots\}=11$. 从而，$\varphi_1$ 在 $\mathcal{U}_S$ 上值为

$$\inf_{a,b}\{(\exists z)\rho(a,b,z)\}=\inf_{a,b}\{11,11,\cdots\}=11.$$

(3.2) 若 $\pi$ 为 $\varphi_2,\cdots,\varphi_5$. 可以仿 (3.1) 验证其在 $\mathcal{U}_S$ 上值为 11，也可仿下面的 (3.4) 证明此事.

(3.3) 若 $\pi\in D$. 再分两种情况.

(3.3.1) 若 $\pi$ 为 $\rho(c_a,c_b,c_c)$ 形状．由 $D$ 的定义知在 $H^*$ 中有 $a\cdot b=c$. 又由 $\pi\in S$ 及 $H$ 的取法可知 $a,b,c\in H$. 所以存在 $i,j,k\in\{1,2,\cdots,n\}$ 能使 $\lambda(i)=a$，$\lambda(j)=b$，$\lambda(k)=c$. 从而有 $\lambda(i)\cdot\lambda(j)=\lambda(k)$，再由 $\lambda_1\supset\lambda$ 及 $\lambda_2\supset\lambda$ 及 $r$ 的定义可知有 $r(i,j,k)=11$. 又易见 $c_a,c_b,c_c$ 在 $\mathcal{U}_S$ 中的解释分别为 $i,j,k$，所以 $\rho(c_a,c_b,c_c)$ 在 $\mathcal{U}_S$ 上的值为 $r(i,j,k)=11$.

(3.3.2) 若 $\pi$ 为 $\neg\rho(c_a,c_b,c_c)$ 形状．由 $D$ 的定义知在 $H^*$ 中有 $a\cdot b\neq c$. 再仿 (3.3.1) 可知 $\rho(c_a,c_b,c_c)$ 在 $\mathcal{U}_S$ 上的值为 00. 所以 $\pi$

在 $\mathcal{U}_S$ 上值为 $(00)' = 11$.

(3.4) 若 $\pi$ 为 $\Pi$. 现在证明它在 $\mathcal{U}_S$ 上的值为 10.

(3.4.1) 由于 $\lambda_1$ 是由 $A_S$ 到 $G_1$ 的 1-1 映射，故知，对任何 $a, b \in A_S$: "$a \equiv b$ 在 $\mathcal{U}_S$ 上值为 11" 当且只当 "$\lambda_1(a) \equiv \lambda_1(b)$ 在 $G_1$ 上值为 $t$(即在 $G_1$ 上为真)". (注意，在 $L$ 值模型上，根据约定，$x \equiv y$ 只取 11 或 00 这两种值.)

(3.4.2) 由 $r$ 的定义可知，对任何 $a, b, c \in A_S$: "$r(a, b, c)$ 在 $\mathcal{U}_S$ 上值为 11 或 10" 当且只当 "$\lambda_1(a) \cdot \lambda_1(b) = \lambda_1(c)$ 在 $G_1$ 上值为 $t$".

(3.4.3) 再注意到 $\lambda_1$ 是到 $G_1$ 上的，并且下列由 4 元布尔代数 $L$ 到 2 元布尔代数 $B = \{t, f\}$ 上的映射 $\mu_1$:

$$11 \to t, \quad 10 \to t, \quad 01 \to f, \quad 00 \to f.$$

是保持运算 $\cap, \cup, '$, 及 inf, sup 的. 由此就不难看出，对 $\mathcal{L}$ 中任何语句 $\sigma$, 都有 (可以对 $\sigma$ 的长度归纳证明): "$\sigma$ 在 $L$ 值模型 $\mathcal{U}_S$ 上值为 11 或 10" 当且只当 "$\sigma$ 在 2 值模型 $G_1$ 上值为 $t$(即在 $G_1$ 上为真)".

特别地，对于语句 $\Pi$ 而言，由于 $G_1$ 适合 $\Pi$, 故有: $\Pi$ 在 $\mathcal{U}_S$ 上值为 11 或 10.

(3.4.4) 考虑由 $A_S$ 到 $G_2$ 上的 1–1 映射 $\lambda_2$, 以及由 $L$ 到 $B$ 上的映射 $\mu_2$:

$$11 \to t, \quad 01 \to t, \quad 10 \to f, \quad 00 \to f.$$

仿照 (3.4.1) 至 (3.4.3) 可以证明: $\Pi$ 在 $\mathcal{U}_S$ 上值为 00 或 10.

(3.4.5) 联合 (3.4.3) 及 (3.4.4) 的二结论即知: $\Pi$ 在 $\mathcal{U}_S$ 上值为 10.

(3.5) 由 (3.1) 至 (3.4) 可知，$\mathcal{U}_S$ 是 $S$ 的 $L$ 值模型. 再由 $S$ 的任意性及关于 $L$ 值模型的紧致性定理 (见第 11 章) 即知: $T$ 具有 $L$ 值模型. 又由 $H^*$ 无限可知 $T$ 的模型都是无限模型，故由 $L$ 值

模型的上升 LST 定理 (见第 11 章) 可知， $T$ 具有基数为 $\alpha$ 的模型 (因 $\alpha \geqslant |H^*| = \|\mathcal{L}_1\|$). 任取其一记为 $\mathcal{U}^*$.

(4) 现在由 $\mathcal{U}^*$ 构作 $\mathcal{L}$ 的两个基数为 $\alpha$ 的 2 值模型 $G_1^*$ 与 $G_2^*$ 如下.

(4.1) 取 $\mathcal{U}^*$ 的论域 $A^*$ 作为 $G_1^*$ 的论域. 并取 $\mathcal{U}^*$ 中对诸 $c_h$ 的解释作为 $G_1^*$ 中对诸 $c_h$ 的解释.

再定义 $G_1^*$ 的 3 元关系 $p_1(a,b,c)$ 如下. 对任何 $a,b,c \in G_1^*$, 令 "$p_1(a,b,c)$ 在 $G_1^*$ 上值为 $t$ (即: 在 $G_1^*$ 上为真)" 当且只当 "$r(a,b,c)$ 在 $\mathcal{U}^*$ 上值为 11 或 10". (其中 $r$ 为 $\mathcal{U}^*$ 中对 $\rho$ 的解释.) 以 $p_1$ 作为 $G_1^*$ 中对 $\rho$ 的解释.

现在根据 $\mathcal{U}^*$ 是 $T$ 的 $L$ 值模型来证明: 当把 $p_1(a,b,c)$ 看作 $a \cdot b = c$ 时， $G_1^*$ 是一个群，它适合 $\Pi$. 并且含有一个与 $H^*$ 同构的子群.

(4.1.1) 任取 $a,b \in G_1^*(= A^*)$. 由 $\varphi_1$ 在 $\mathcal{U}^*$ 上值为 11 可知, $(\exists z)\rho(a,b,z)$ 在 $\mathcal{U}^*$ 上值为 11, 也即 $\sup\limits_z\{r(a,b,z)\} = 11$. 由此可知, 存在 $c \in A^*$ 能使 $r(a,b,c)$ 在 $\mathcal{U}^*$ 上值为 11 或 10, 从而 $p_1(a,b,c)$ 在 $G_1^*$ 上为真. 所以， $G_1^*$ 对于由 $p_1$ 所决定的乘法封闭.

(4.1.2) 再根据 $\varphi_2,\cdots,\varphi_5$ 在 $\mathcal{U}^*$ 上值都为 11 的事实，可以仿 (4.1.1) 证明，也可以仿下面的 (4.1.4) 证明： $G_1^*$ 对于由 $p_1$ 所决定的乘法构成一个群.

(4.1.3) 由于 $G_1^*$ 中对诸 $c_h$ 的解释与 $\mathcal{U}^*$ 中相同，而 $D$ 中诸语句在 $\mathcal{U}^*$ 中的值都是 11, 再对照 $G_1^*$ 的 3 元关系 $p_1$ 的定义以及 $D$ 的定义，就可看出： $G_1^*$ 含有一个与 $H^*$ 同构的子群.

(4.1.4) 令 $\lambda_1$ 为由 $A^*$ 到 $G_1^*(= A^*)$ 上的恒等映射. 则仿照 (3.4.1) 至 (3.4.3) 可以证明，对 $\mathcal{L}$ 中任何语句 $\sigma$ 都有： "$\sigma$ 在 $\mathcal{U}^*$ 上值为 11 或 10" 当且只当 "$\sigma$ 在 $G_1^*$ 上为真". 特别地，由于语句 $\Pi$ 在 $\mathcal{U}^*$ 上值为 10, 所以 $\Pi$ 在 $G_1^*$ 上为真，也即 $G_1^*$ 适合性质 $P$.

(4.2) 取 $A^*$ 作为 $G_2^*$ 的论域. 并取 $\mathcal{U}^*$ 中对诸 $c_h$ 的解释作为 $G_2^*$ 中对诸 $c_h$ 的解释.

再定义 $G_2^*$ 的 3 元关系 $p_2(a,b,c)$ 如下. 对任何 $a,b,c\in G_2^*$, 令 "$p_2(a,b,c)$ 在 $G_2^*$ 上值为 $t$" 当且只当 "$r(a,b,c)$ 在 $\mathcal{U}^*$ 上值为 11 或 01".

仿照 (4.1) 可以证明: 当把 $p_2(a,b,c)$ 看作 $a\cdot b=c$ 时, $G_2^*$ 是一个群, 它不适合 $\Pi$(也即不适合性质 $P$), 并且含有一个与 $H^*$ 同构的子群. (证毕)

上定理中的 "两个扩群" 可以推广到 "$n$ 个扩群" 各适合或不适合某些 1 阶性质的情况 (用 $2^n$ 元布尔代数作为值格 $L$ 仿上证明). 此外, 上定理中的 "群"、"可换群" 等字样也可以换为其他代数结构, 仍有类似的结论成立.

另外, 也可以用 2 值逻辑的紧致性定理来证明上定理, 但需要: 或者用比 $\mathcal{L}_1$ 更复杂的语言以及比 $T$ 更复杂的理论; 或者用两次紧致性定理 (在 $n$ 个扩群的情况则是用 $n$ 次), 并且设法说明所存在的 $G_1^*$ 及 $G_2^*$(在 $n$ 个扩群的情况则是 $G_1^*$ 及 $\cdots$ 及 $G_n^*$) 是同一个 $H^*$ 的扩群. 所以, 2 值逻辑的证法与 $L$ 值逻辑的证法各有短长.

**3.3** 最后, 再附述一个 $L_2$ 值逻辑应用的例.

**定理 5** 令 $L$ 为 2 人知识状态值格 $K_2$. 设 $\mathcal{L}$ 为任一语言, $p,q_1,q_2,\cdots,q_i,\cdots$($i$ 通过一切正整数) 为 $\mathcal{L}$ 中的语句. 如果对每个正整致 $r$ 都存在 $\mathcal{L}$ 的 $L$ 值模型 $\mathcal{U}_r$ 能使 $q_1,\cdots,q_r$ 在 $\mathcal{U}_r$ 上值均为 11 而 $p$ 在 $\mathcal{U}_r$ 上值为 $1n$, 则:

(1) 对每个正整致 $r$ 都有

(1.1) 在 2 值逻辑中, $q_1\wedge\cdots\wedge q_r\not\vdash\neg p$.

(1.2) $p$ 不能表示为 $q_1,\cdots,q_r$ 的任何布尔表达式.

(2) 存在 $\mathcal{L}$ 的 $L$ 值模型 $\mathcal{U}$, 能使 $q_1,q_2,\cdots,q_i,\cdots$ 在 $\mathcal{U}$ 上值均为 11 而 $p$ 在 $\mathcal{U}$ 上值为 $1n$.

**证明** (1.1) 由题设知，在 $\mathcal{U}_r$ 上，$(q_1 \wedge \cdots \wedge q_r) \to \neg p$ 的值为

$$(11 \cap \cdots \cap 11)' \cup (1n)' = 0n < nn,$$

故由定理 1.2 知 $(q_1 \wedge \cdots \wedge q_r) \to \neg p$ 不是 2 值逻辑的恒真式，从而 $q_1 \wedge \cdots \wedge q_r \nvdash \neg p$.

(1.2) 假若 $p$ 能表示为 $q_1, \cdots, q_r$ 的布尔表达式，则由 $q_1, \cdots, q_r$ 在 $\mathcal{U}_r$ 上值均为 11 及格 $K_2$ 的运算表易见 $p$ 在 $\mathcal{U}_r$ 上的值应为 11 或 00, 与题设矛盾.

(2) 令 $T$ 为 $\mathcal{L}$ 中的下列理论

$$T = \{q_1, q_2, \cdots, q_i, \cdots\}_{11} \cup \{p\}_{1n},$$

对 $T$ 引用 $L$ 值逻辑的紧致性定理即可. (证毕)

上定理中的 "$1n$" 也可都改为 "$n1$", 证法完全类似.

## 参考文献


1 王世强. 格值模型论中紧致性定理的一种证法. 北京师范大学学报, 1980(3~4): 25~30

2 王世强, 吴望名. 可补格按恒 I 式集分类的问题. 北京师范大学学报, 1964(2): 125~133

# 第 10 章

# 格值谓词演算中的标准形

本章讨论某些格值谓词演算中的前束标准形及 Skolem 标准形. 它们有助于考虑这些格值逻辑中的判定问题及模型论问题.

我们对值格 $L$ 要考虑下列诸性质:

**性质 ($\mathbf{F}_1$)** 对 $L$ 的每一非空子集 $M$, 都存在有限个元 $x_1, \cdots, x_k \in M$($k$ 与 $M$ 有关) 能使

$$x_1 \cup \cdots \cup x_k = \sup_{x \in M} x.$$

**性质 ($\mathbf{F}_1^\circ$)** 存在一正整数 $k$, 使对 $L$ 的每一非空子集 $M$ 都存在 $x_1, \cdots, x_k \in M$(不论同异) 能使

$$x_1 \cup \cdots \cup x_k = \sup_{x \in M} x.$$

**性质 ($\mathbf{F}_2$)** 对 $L$ 的每一非空子集 $M$, 都存在有限个元 $x_1, \cdots, x_l \in M$ ($l$ 与 $M$ 有关) 能使

$$x_1 \cap \cdots \cap x_l = \inf_{x \in M} x.$$

**性质 ($\mathbf{F}_2^\circ$)** 存在一正整数 $l$, 使对 $L$ 的每一非空子集 $M$ 都存在 $x_1,\cdots,x_l\in M$(不论同异) 能使

$$x_1\cap\cdots\cap x_l=\inf_{x\in M}x.$$

**性质 (D)** 对 $L$ 的每一非空子集 $M$, 都有

$$(\sup_{x\in M}x)'=\inf_{x\in M}(x');\quad (\inf_{x\in M}x)'=\sup_{x\in M}(x').$$

**性质 ($\mathbf{D}^\circ$)** 对任何 $x,y\in L$, 都有

$$(x\cup y)'=x'\cap y';\quad (x\cap y)'=x'\cup y'.$$

性质 ($\mathrm{F}_1^\circ$),($\mathrm{F}_2^\circ$) 及 ($\mathrm{D}^\circ$) 显然分别是性质 ($\mathrm{F}_1$), ($\mathrm{F}_2$) 及 (D) 的特例.

有不少关于格值逻辑的结论, 对于适合 ($\mathrm{F}_1$) 及 ($\mathrm{F}_2$) 的值格 $L$ 都能成立, 但对于适合 ($\mathrm{F}_1^\circ$) 及 ($\mathrm{F}_2^\circ$) 的 $L$ 在叙述及论证上更方便些. 作者在有些文献中采用后一形式, 是高恒珊先生向作者建议了前一种更一般的形式.

又, 适合性质 (D) 的格 $L$ 未必是完备布尔代数. 例如上一章定理 3 的证明中所用的格 $L$, 它适合 (D) 但不是布尔代数. 其他的例还有很多.

**引理 1** 若完备可补格适合性质 ($\mathrm{F}_1$),($\mathrm{F}_2$) 及 ($\mathrm{D}^\circ$), 则 $L$ 适合性质 (D).

**证明** 任取 $L$ 的非空子集 $M$, 令 $M'=\{x':\ x\in M\}$, 则由 ($\mathrm{F}_1$) 及 ($\mathrm{F}_2$) 知存在 $x_1,\cdots,x_k\in M$ 及 $x_{k+1},\cdots,x_{k+l}\in M$ 能使 $\sup\limits_{x\in M}x=x_1\cup\cdots\cup x_k$ 及 $\inf\limits_{x\in M}(x')=\inf\limits_{x'\in M'}(x')=x'_{k+1}\cap\cdots\cap x'_{k+l}$, 从而再由 ($\mathrm{D}^\circ$) 可得

$$\begin{aligned}\Big(\sup_{x\in M}x\Big)'&=(x_1\cup\cdots\cup x_k)'=(x_1\cup\cdots\cup x_k\cup\cdots\cup x_{k+l})'\\&=x'_1\cap\cdots\cap x'_k\cap\cdots\cap x'_{k+l}=x'_1\cap\cdots\cap x'_k\cap\inf_{x\in M}(x')=\inf_{x\in M}(x').\end{aligned}$$

仿此也可证明 (D) 中另一等式.　　　(证毕)

以下为了方便，在写合式公式时，把逻辑符号 $\wedge, \vee, \neg, \exists, \forall$ 及其 $L$ 值的解释 $\cap, \cup, ', \sup, \inf$ 两者通用.

## §1　前束标准形

**引理 2**　当值格 $L$ 适合 $(F_1^\circ)$ 时，在 $L$ 值谓词演算中有下列等值式成立：

$$
\begin{aligned}
\text{(e)}\quad & \left\{\left[\sup_{x_1}\cdots\sup_{x_r} A(x_1,\cdots,x_r)\right]\cap B\right\} \\
&= \sup_{x_{11}}\cdots\sup_{x_{1r}}\sup_{x_{21}}\cdots\sup_{x_{2r}}\cdots\sup_{x_{k1}}\cdots\sup_{x_{kr}}\{[A(x_{11},\cdots,x_{1r}) \\
&\quad \cup A(x_{21},\cdots,x_{2r})\cup\cdots\cup A(x_{k1},\cdots,x_{kr})]\cap B\}.
\end{aligned}
$$

其中 $k$ 为性质 $(F_1^\circ)$ 中所说的正整数； $r$ 为任一正整数； $A,B$ 是任意合式公式，但满足一些明显的技术性条件 (即： $x_{11},\cdots,x_{kr}$ 不在 $A(x_1,\cdots,x_r)$ 中或 $B$ 中自由出现； $x_1,\cdots,x_r$ 在 $A$ 中的自由出现不在含 $x_{11}$ 或 $\cdots$ 或 $x_{kr}$ 的量词范围内. 这类条件以后都不详述); 等号则表示在任何解释之下，其左右两端所得的 $L$ 值都相同.

**证明**　任取一非空集 $S$, 在 $S$ 中任取一组元素来解释 (e) 中的自由变元，并任取 $S$ 上的一组 $L$ 值谓词 (也即 $L$ 值关系) 来解释 (e) 中的谓词变元 (包括命题变元，即 0 元谓词变元). 这样取定的一种解释方式 $V$ 以下称为 (e) 的一个赋值. 在 $V$ 下，设 (e) 式等号左端值为 $\lambda$, 右端值为 $\mu$.

(1) 由于对任何 $a_{11},\cdots,a_{kr}\in S$ 都有

$$
\begin{aligned}
&\{[A(a_{11},\cdots,a_{1r})\cup\cdots\cup A(a_{k1},\cdots,a_{kr})]\cap B\} \\
&\quad \leqslant \{[\sup_{x_1}\cdots\sup_{x_r} A(x_1,\cdots,x_r)]\cap B\} = \lambda,
\end{aligned}
$$

所以易见有 $\mu \leqslant \lambda$.

(2) 设在 $V$ 下 $\sup\limits_{x_1}\cdots\sup\limits_{x_r} A(x_1,\cdots,x_r)$ 值为 $\rho$, $B$ 值为 $\sigma$. 由 $L$ 的性质 $(\mathrm{F}_1^\circ)$ 可知 (以 $\{A(a_1,\cdots,a_r):\ a_1,\cdots,a_r\in S\}$ 作为 $L$ 的子集 $M$) 存在 $a_{11},\cdots,a_{kr}\in S$ 能使

$$A(a_{11},\cdots,a_{1r})\cup\cdots\cup A(a_{k1},\cdots,a_{kr})=\rho,$$

从而 $\{[A(a_{11},\cdots,a_{1r})\cup\cdots\cup A(a_{k1},\cdots,a_{kr})]\cap B\}=\rho\cap\sigma=\lambda$, 所以易见有 $\mu\geqslant\lambda$. (证毕)

以下为了书写方便, 我们引入一些简记法: 把变元序组 $x_1,\cdots,x_r$ 简记为 $\overline{x}$, 把 $\sup\limits_{x_1}\cdots\sup\limits_{x_r}$ 简记为 $\sup\limits_{\overline{x}}$, 等等. (其中 $r$ 为任意, 并且在不同的符号 $\overline{x},\overline{x}_1,\cdots$ 中其值可以不同, 因一般不致引起误解, 故不在简记号中表明.) 这时, 引理 2 中的 (e) 式就可简记为

$$\{[\sup_{\overline{x}} A(\overline{x})]\cap B\}=\sup_{\overline{x}_1}\cdots\sup_{\overline{x}_k}\{[A(\overline{x}_1)\cup\cdots\cup A(\overline{x}_k)]\cap B\}.$$

**引理 3** 当值格 $L$ 适合 $(\mathrm{F}_2^\circ)$ 时, 在 $L$ 值谓词演算中有下列等值式成立:

$$\{[\inf_{\overline{x}} A(\overline{x})]\cup B\}=\inf_{\overline{x}_1}\cdots\inf_{\overline{x}_l}\{[A(\overline{x}_1)\cap\cdots\cap A(\overline{x}_l)]\cup B\}.$$

证明仿引理 2, 略去.

对每一非负整数 $p$, 我们用 $(Q_{s,p})$ 表示如下形状的一串量词 ($p=0$ 时量词串为空)

$$\sup_{\overline{x}_1}\inf_{\overline{x}_2}\sup_{\overline{x}_3}\inf_{\overline{x}_4}\cdots\begin{cases}\sup\limits_{\overline{x}_p} & \text{当 } p \text{ 为奇},\\ \inf\limits_{\overline{x}_p} & \text{当 } p \text{ 为偶}.\end{cases}$$

用 $(Q_{i,p})$ 表示

$$\inf_{\overline{x}_1}\sup_{\overline{x}_2}\inf_{\overline{x}_3}\sup_{\overline{x}_4}\cdots\begin{cases}\inf_{\overline{x}_p} & \text{当 } p \text{ 为奇,}\\ \sup_{\overline{x}_p} & \text{当 } p \text{ 为偶.}\end{cases}$$

$p$ 称为量词串的长度.（注意 $p$ 一般不是量词串中量词的个数，而是两类量词交替的次数.）

**引理 4** 当值格 $L$ 适合 $(F_1^\circ)$ 及 $(F_2^\circ)$ 时，$L$ 值谓词演算中每一个由若干子式 $(Q_{t,p})G_1,\cdots,(Q_{t,p})G_n$（$t$ 代表 $s$ 或 $i$; $t,p$ 在各式中都相同）经 $\cap,\cup$ 组成的合式公式 $P_1((Q_{t,p})G_1,\cdots,(Q_{t,p})G_n)$ 都能有效地化为一个等值的合式公式 $(Q_{t,p})P_2(G_1,\cdots,G_n)$, 其中 $P_2$ 是由 $G_1,\cdots,G_n$ 经 $\cap,\cup$ 组成的.

**证明** 对 $p$ 归纳. 当 $p=0$ 时，取 $P_2$ 为 $P_1$ 即可.

设 $p\leqslant k$ 时引理已成立，当 $p=k+1$ 时,

再对 $P_1$ 中 $\cap,\cup$ 的个数 $d$ ($G_1,\cdots,G_n$ 内的 $\cap,\cup$ 不计) 归纳:

当 $d=0$ 时，$P_1=(Q_{t,k+1})G_1$, 取 $P_2$ 为 $G_1$ 即可.

设 $d\leqslant h$ 时引理已成立，当 $d=h+1$ 时:

(1) 若 $P_1=P_{11}\cap P_{12}$. 由关于 $d$ 的归纳假设知 $P_{11}$, $P_{12}$ 各可有效地化为等值的 $(Q_{t,k+1})P_{21},(Q_{t,k+1})P_{22}$, 其中 $P_{21},P_{22}$ 都是由 $G_1,\cdots,G_n$ 经 $\cap,\cup$ 组成的.

(1.1) 当 $t$ 为 $s$ 时: $P_1$ 等值于 $(Q_{s,k+1})P_{21}\cap(Q_{s,k+1})P_{22}$, 此式又可写为

$$\sup(Q_{i,k})P_{21}\cap\sup(Q_{i,k})P_{22},$$

(其中两个 sup 下面应附的个体变元组未必相同，因对论证无关紧要，故略而不写. 以下仿此.) 连用两次引理 2, 可将上式化为 sup $P_3$ 形状，其中 $P_3$ 由 $(Q_{i,k})P_{21},(Q_{i,k})P_{22}$ 经 $\cap,\cup$ 构成. 再由关于 $p$ 的归纳假设，知 $P_3$ 可有效地化为 $(Q_{i,k})P_4$ 形状，其中 $P_4$ 由 $P_{21},P_{22}$

经 $\cap,\cup$ 组成. 因而 $P_1$ 等值于 $\sup(Q_{s,k})P_4$, 也即 $(Q_{s,k+1})P_4$. $P_4$ 即可充当引理中所说的 $P_2$.

(1.2) 当 $t$ 为 $i$ 时: $P_1$ 等值于 $(Q_{i,k+1})P_{21}\cap(Q_{i,k+1})P_{22}$. 此式又可写为

$$\inf(Q_{s,k})P_{21}\cap\inf(Q_{s,k})P_{22}.$$

由格性质知上式等值于 $\inf[(Q_{s,k})P_{21}\cap(Q_{s,k})P_{22}]$, 再对 $[\cdots]$ 部分应用关于 $p$ 的归纳假设即可.

(2) 若 $P_1=P_{11}\cup P_{12}$. 仿 (1). (代替引理 2 而用引理 3.) (证毕)

**定理 1** (前束标准形定理) 当值格 $L$ 适合 $(\mathrm{F}_1^\circ)$,$(\mathrm{F}_2^\circ)$ 及 $(\mathrm{D}^\circ)$ 时, 对 $L$ 值谓词演算中任一合式公式 $A$ 都可有效地化为一个等值的前束标准形 $B$.

**证明** 由引理 2.1 知 $L$ 适合 (D), 故可先对 $A$ 作等值变形, 使每个连接词 "′" 的辖域内都无量词出现. (在任何赋值 $V$ 之下, (D) 中所说 $L$ 的子集 $M$ 都可适当选择, 不详述.) 再通过多余量词的引入 (例如, 可将 $\sup\limits_{x}\inf\limits_{y}\sup\limits_{z} A_1\cap\inf\limits_{v} A_2$ 中的第二项换为等值的 $\sup\limits_{u}\inf\limits_{v}\sup\limits_{w} A_2$, 其中 $u,w$ 为不在 $A_2$ 中出现的个体变元), 即可陆续应用引理 2.4 若干次而得一个等值的前束标准形 $B$. (证毕)

## §2 Skolem 标准形

设 $C(p,q)$ 是一个命题演算合式公式, $L$ 是一个有补运算的格. 如果对任何 $a,b\in L$ 都有

$$C(a,b)=\begin{cases}I, & 若\ a=b;\\ 0, & 若\ a\neq b.\end{cases}$$

则称 $C(p,q)$ 为 $L$ 的一个 **特征式**(或称 **强特征式**). 如果对任何

$a,b \in L$ 都有

$$C(a,b) \begin{cases} = I, & 若\ a = b; \\ \neq I, & 若\ a \neq b. \end{cases}$$

则称 $C(p,q)$ 为 $L$ 的一个 **弱特征式**.

例如，若 $L$ 是一个布尔代数，则

$$(p' \cup q) \cap (p \cup q')$$

是 $L$ 的一个弱特征式. 容易证明，对于元数大于 2 的布尔代数，不存在强特征式.

又如，若 $L$ 是上一章定理 3 的证明中所用的格，则

$$(p' \cup q) \cap (p \cup q') \cap ((p' \cup q) \cap (p \cup q'))''$$

是 $L$ 的一个强特征式.

**引理 5** 当值格适合 $(\mathrm{F}_1^\circ)$,$(\mathrm{F}_2^\circ)$,$(\mathrm{D}^\circ)$ 且具有弱特征式 $C(p,q)$ 时，对谓词演算中任一合式公式 $G(x_1,\cdots,x_r,y_1,\cdots,y_s)$(以下简记为 $G(\overline{x},\overline{y})$)，下列二条件等价：

(a) $\sup\limits_{\overline{x}} \inf\limits_{\overline{y}} G(\overline{x},\overline{y})$ 恒不为 0;（指：在任何赋值之下，其值都不为 0. 以下仿此.）

(b) $\sup\limits_{\overline{x}} \sup\limits_{\overline{y}}[(C(G(\overline{x},\overline{y}),H(\overline{x},\overline{y})))' \cup \inf\limits_{\overline{z}} H(\overline{x},\overline{z})]$ 恒不为 0. 其中 $H$ 为任一不出现于 $G$ 中的 $r+s$ 元谓词变元.

**证明** (1) 设 (a) 成立. 考虑 (b) 中公式的任一赋值 $V$.（设 $V$ 所用的非空集为 $S$.）

(1.1) 在 $V$ 下，若存在 $a_1,\cdots,a_r,b_1,\cdots,b_s \in S$ 能使 $G(\overline{a},\overline{b}) \neq H(\overline{a},\overline{b})$，则 $(C(G(\overline{a},\overline{b}),H(\overline{a},\overline{b})))' \neq 0$，从而易见 (b) 中公式的值不为 0.

(1.2) 在 $V$ 下，若 $G(\overline{x},\overline{y})$ 与 $H(\overline{x},\overline{y})$ 的值永相同，则 (b) 中公

式的值为

$$\sup_{\overline{x}}\sup_{\overline{y}}[0\cup\inf_{\overline{z}} G(\overline{x},\overline{z})]=\sup_{\overline{x}}\inf_{\overline{z}} G(\overline{x},\overline{z}),$$

故由 (a) 知其不为 0.

(2) 设 (b) 成立. 考虑 (a) 中公式的任一赋值 $V$. 现在用 $V$ 解释 (b) 中公式, 并将 (b) 中的 $H$ 解释为

$$H(\overline{x},\overline{y})=G(\overline{x},\overline{y}) \text{ 在 } V \text{ 下的值},$$

则 (b) 中公式的值为

$$\sup_{\overline{x}}\sup_{\overline{y}}[0\cup\inf_{\overline{z}} G(\overline{x},\overline{z})]=\sup_{\overline{x}}\inf_{\overline{z}} G(\overline{x},\overline{z}),$$

此式右端即为 (a) 中公式在 $V$ 下的值, 故由 (b) 知此值不为 0. (证毕)

**定理 2** 当值格 $L$ 适合 $(F_1^\circ)$,$(F_2^\circ)$,$(D^\circ)$ 且具有弱特征式 $C(p,q)$ 时, 对 $L$ 值谓词演算中任一合式公式 $A$ 都可有效地找到一个形状为

$$\sup_{\overline{x}}\inf_{\overline{y}} K(\overline{x},\overline{y}) \quad (K \text{ 中不含量词})$$

的合式公式 $B$ (称为 Skolem 标准形) 使: $A$ 恒不为 0 当且只当 $B$ 恒不为 0.

**证明** 首先, 由定理 2.1 可有效地找到一个与 $A$ 等值的前束标准形 $A_1$, 并且不妨设 $A_1$ 为 $(Q_{s,n})M$ 形状, 其中 $n\geqslant 2$, $M$ 不含量词.

若 $n=2$, $A_1$ 即为所求. 以下对 $n$ 归纳. 设 $n\leqslant k$ 时已真 $(k\geqslant 2)$, 当 $n=k+1$ 时:

注意到 $C(p,q)$ 是由 $p,q$ 经 $\cap,\cup,'$ 组成的, 利用 $(D^\circ)$ 可将 $(C(p,q))'$ 等值地化为 $P(p,p',p'',\cdots,q,q',q'',\cdots)$ 形状, 其中 $P$ 是由 $p,p',p'',\cdots,q,q',q'',\cdots$ 经 $\cap,\cup$ 组成的.

由于 $A_1 = (Q_{s,k+1})M = \sup\inf(Q_{s,k-1})M$, 故由引理 5 可有效地找到

$$B_1 = \sup\sup[(C((Q_{s,k-1})M, H))' \cup \inf\ H]$$

使： $A_1$ 恒不为 0 当且只当 $B_1$ 恒不为 0.

但 $B_1$ 又等值于

$$\sup\sup[P((Q_{s,k-1})M, (Q_{i,k-1})M', (Q_{s,k-1})M'', \\ \cdots, H, H', H'', \cdots) \cup \inf\ H],$$

通过多余量词的引入, 上式中的 $(Q_{s,k-1}), (Q_{i,k-1})$ 都可化为 $(Q_{s,k})$, 再由引理 4 可将上式等值地化为

$$\sup\sup[(Q_{s,k})P_1 \cup \inf\ H],$$

再由同样理由，此式又可等值地化为

$$\sup\sup(Q_{s,k})P_2\ (\text{记作}\ B_2).$$

$B_2$ 为 $(Q_{s,k})M_1$ 形状 ($M_1$ 不含量词). 再应用归纳假设，由 $B_2$ 能有效地找到一个 Skolem 标准形 $B$ 使： $B_2$ 恒不为 0 当且只当 $B$ 恒不为 0.

综合上述即知, 当 $n = k+1$ 时定理也成立. 归纳完成. (证毕)

**定理 3** 当值格 $L$ 适合 $(\mathrm{F}_1^\circ)$,$(\mathrm{F}_2^\circ)$,$(\mathrm{D}^\circ)$ 且具有强特征式 $C(p,q)$ 时，对 $L$ 值谓词演算中任一合式公式 $A$ 都可有效地找到一个形状为

$$\sup_{\overline{x}}\ \inf_{\overline{y}}\ K(\overline{x}, \overline{y})\quad (K\ \text{中不含量词})$$

的合式公式 $B$(称为 Skolem 标准形) 使： $A$ 为恒 $I$ 式当且只当 $B$ 为恒 $I$ 式.

证明仿引理 5 及定理 2, 略去.

当值格 $L$ 为元数大于 2 的布尔代数时, 虽然 $L$ 不具有强特征式, 但定理 3 的结论仍成立.

## §3 Löwenheim 定理

本节附述某些值格时 Löwenheim 定理的一些初步形式, 它们是下一章中 LST 定理的特例.

**定理 4** 设 $A$ 为谓词演算中一个 Skolem 标准形的语句, 并且值格 $L$ 适合 $(F_2^\circ)$. 在 $L$ 值逻辑中, 若 $A$ 不为恒 $I$ 式, 则 $A$ 在正整数集 $\mathbf{N}$ 上不为恒 $I$ 式.

**证明** 设 $A=(\exists x_1\cdots x_m)(\forall y_1\cdots y_n)B(x_1,\cdots,x_m,y_1,\cdots,y_n)$, 其中 $m\geqslant 0$, $n\geqslant 0$; $x_1,\cdots,x_m,y_1,\cdots,y_n$ 互异; $B$ 中无量词, 也不含其他个体变元.

(甲) 若 $A$ 在某个无限集 $D$ 上不为恒 $I$ 式.

以下为使记号简单, 以 $m=2,n=3$ 为例来说明一般思路.

由题设 (甲) 知, 存在 $A$ 在 $D$ 上的赋值 $V$, 使 $A$ 在 $V$ 下的值 $\alpha<I$. 在 $V$ 下有

$$\alpha=\sup_{x_1,x_2\in D}\inf_{y_1,y_2,y_3\in D}B(x_1,x_2,y_1,y_2,y_3) \tag{1}$$

(I) 任意取定一组 $a_1,a_2\in D$, 则由 (1) 有

$$\inf_{y_1,y_2,y_3\in D}B(a_1,a_2,y_1,y_2,y_3)=\beta\leqslant\alpha,$$

也即

$$\inf_{y_1\in D}(\inf_{y_2,y_3\in D}B(a_1,a_2,y_1,y_2,y_3))=\beta\leqslant\alpha.$$

由 $(F_2^\circ)$ 可知, 存在 $b_1,\cdots,b_l\in D$ 能使

$$\inf_{y_2,y_3\in D}B(a_1,a_2,b_1,y_2,y_3)\cap\cdots\cap\inf_{y_2,y_3\in D}B(a_1,a_2,b_l,y_2,y_3)=\beta.$$

再对此式左端每项反复用同样论证，即可见在 $D$ 中存在 $l+l^2+l^3$ 个元（不论同异）$b_i, b_{ij}, b_{ijk}$ $(1 \leqslant i, j, k \leqslant l)$ 能使

$$\inf_{1\leqslant i,j,k\leqslant l} B(a_1, a_2, b_i, b_{ij}, b_{ijk}) \leqslant \alpha. \tag{2}$$

(2.1) 任意取定一个元 $d \in D$. 根据 (1) 任意取定 $D$ 中 $l+l^2+l^3$ 个元 $b_i, b_{ij}, b_{ijk}$ 使适合

$$\inf_{1\leqslant i,j,k\leqslant l} B(d, d, b_i, b_{ij}, b_{ijk}) \leqslant \alpha.$$

再任意取定 $D$ 中一个 $\neq d$ 的元 $d_1$, 令

$$D_1 = \{d, d_1, b_i, b_{ij}, b_{ijk}\}.$$

(2.2) 对每一组 $a_1, a_2 \in D_1$, 都根据 (1) 任意取定 $D$ 中 $l+l^2+l^3$ 个 $b_i, b_{ij}, b_{ijk}$ 使适合 (2). 把所有这些元都加入 $D_1$ 中；再任意取定 $D$ 中一个 $\neq d, d_1$ 的元 $d_2$, 也加入 $D_1$ 中；这样得 $D$ 的子集 $D_2$. 并且，由 $D_1$ 有限可知 $D_2$ 有限，其元数 $> 2$.

(2.3) 再仿 (2.2) 进行：把 $D_2$ 扩张为 $D$ 的有限子集 $D_3$, 其元数 $> 3$; 把 $D_3$ 扩张为 $D$ 的有限子集 $D_4$, 其元数 $> 4$;$\cdots\cdots$. 最后，令

$$\overline{D} = \bigcup_{r\in\mathbf{N}} D_r,$$

则 $\overline{D}$ 是 $D$ 的一个可数无限子集.

(III) 由 $\overline{D}$ 定义易知：对每一组 $a_1, a_2 \in \overline{D}$, 都存在 $l+l^2+l^3$ 个 $\overline{D}$ 中的元 $b_i, b_{ij}, b_{ijk}$ 能使 (2) 成立，从而有

$$\inf_{y_1,y_2,y_3\in\overline{D}} B(a_1, a_2, y_1, y_2, y_3) \leqslant \alpha.$$

再由 $a_1, a_2$ 在 $\overline{D}$ 中的任意性即知

$$\sup_{x_1,x_2\in\overline{D}} \inf_{y_1,y_2,y_3\in\overline{D}} B(x_1, x_2, y_1, y_2, y_3) \leqslant \alpha < I.$$

所以：$A$ 在可数无限集 $\overline{D}$ 上不为恒 $I$ 式，从而显见 $A$ 在正整数集 $\mathbf{N}$ 上不为恒 $I$ 式.

(乙) 若 $A$ 在某个有限集 $\overline{D}$ 上不为恒 $I$ 式.

不妨设 $D$ 为 $\{1,2,\cdots,k\}$. 由 (乙) 知 $A$ 在以 $D$ 为论域的某赋值 $U$ 下的值 $\alpha < I$. 现在，把正整数集 $\mathbf{N}$ 中每个大于 $k$ 的数都看作"等同"于 $k$, 这样就可模仿 $U$ 找到 $A$ 的一个以 $\mathbf{N}$ 为论域的赋值 $V$, 使 $A$ 在 $V$ 下的值也是 $\alpha$.(注意 $A$ 中不含等号.) 所以，$A$ 在 $\mathbf{N}$ 上不为恒 $I$ 式. (证毕)

**定理 5** 设 $A$ 为谓词演算中一个前束标准形的语句，并且值格 $L$ 适合 $(\mathrm{F}_1^\circ)$ 及 $(\mathrm{F}_2^\circ)$. 在 $L$ 值逻辑中，若 $A$ 不为恒 $I$ 式，则 $A$ 在正整数集 $\mathbf{N}$ 上不为恒 $I$ 式.

证明的思路与定理 4 者类似，略去.

## 参考文献

1 王世强，翁稼丰. 一些多值狭义谓词演算中的标准形. 北京师范大学学报，1980(2): 19～23

# 第 11 章

# 格值模型的紧致性定理

在格值逻辑的模型理论中，有一条基础性的紧致性定理，它对于任何有限的值格都能成立.（可以用超积方法证明此事，见文献 [3].）在本章中，我们用 [2] 中的“常元构作法”来证明在某些特殊的有限值格时的紧致性定理. 我们这样作的目的是为了说明这种有用的方法.

为了便于讨论和行文简单，我们以文献 [1] 作为 2 值模型论的主要参考书 (以后简称 MT), 所采用的术语、符号基本上依据此书. 凡是与此书类似的论证一般都从略，主要只叙述多值时与 2 值不同的那些部分.

设值格 $L=\{\lambda_0,\lambda_1,\lambda_2,\cdots\}$, 其中 $\lambda_0=O$, $\lambda_1=I$.

设 $\mathcal{L}$ 为一语言， $\Sigma$ 为 $\mathcal{L}$ 中任一非空语句集. 将 $\Sigma$ 依任一方式划分为互不相交的子集 $\Sigma_{\lambda_1},\Sigma_{\lambda_2},\cdots$ (可有某些 $\Sigma_{\lambda_j}$ 为空集，又注意划分中无 $\Sigma_{\lambda_0}$). 我们把 $\Sigma$ 连同一个这样的划分称为一个分组语句集成 **理论**, 一般仍记作 $\Sigma$.（注意：同一语句集若作了不同的划分，则看作不同的理论. 必要时在记号上加以区分.）

关于 $\mathcal{L}$ 的模型 $\mathcal{U}$, 其定义与 2 值时类似，只是 $\mathcal{U}$ 中的关系可以取 $L$ 中的任何元为值.（注意，对于等词 $\equiv$ 的取值，与 2 值时

相同. 即：对于 $\mathcal{U}$ 的论域中任二元 $a,b$, 若 $a=b$, 则 $a\equiv b$ 取值 I; 若 $a\neq b$, 则 $a\equiv b$ 取值 O.)

$\mathcal{L}$ 中一语句 $\varphi$ 在 $\mathcal{U}$ 上的值，有时记作 $\varphi|_{\mathcal{U}}$.

设 $\Sigma$ 为 $\mathcal{L}$ 中一个理论，$\mathcal{U}$ 为 $\mathcal{L}$ 的一个模型. 如果对于 $\Sigma$ 的每一子集 $\Sigma_{\lambda_j}$ $(j=1,2,\cdots)$ 中的每一语句 $\varphi$, 都有 $\varphi|_{\mathcal{U}}=\lambda_j$, 则称 $\mathcal{U}$ 满足 $\Sigma$, 也称 $\mathcal{U}$ 是 $\Sigma$ 的一个 **模型**, 记作 $\mathcal{U}\models\Sigma$.

设 $\Sigma$ 为 $\mathcal{L}$ 中一个理论. 若 $\Sigma$ 的每一有限子理论都有模型，则称 $\Sigma$ 为 **有限和谐** 的. (注：$\mathcal{L}$ 中的两个理论 $\Sigma_1,\Sigma_2$ 如果适合 (i) $\Sigma_1\subseteq\Sigma_2$ 及 (ii) $\Sigma_1$ 中每一语句 $\varphi$ 在 $\Sigma_1$ 的分组中的足码与在 $\Sigma_2$ 的分组中的足码相同，则称 $\Sigma_1$ 为 $\Sigma_2$ 的子理论.)

**引理 1** $\mathcal{L}$ 中任一有限和谐的理论 $T$ 都能扩充为一个极大的有限和谐理论.

证明与 MT 中命题 1.3.11 者类似，略去.

以下我们仿照 Henkin 的方法证明：在值格有限且具有弱特征式时，紧致性定理成立.

设值格 $L$ 适合 $(F_1^\circ)$ 及 $(F_2^\circ)$(见第 10 章), 并具有弱特征式 $\Delta(p,q)$. 设 $T$ 为语言 $\mathcal{L}$ 中一个理论，$C$ 为由 $\mathcal{L}$ 中若干个体常元所组成的一个集合. 当下列二条件都成立时，称 $C$ 为 $T$ 在 $\mathcal{L}$ 中的一组 **见证**: 对 $\mathcal{L}$ 中每个至多含 1 个自由变元的合式公式 $\varphi(x)$,

$(\mathrm{W}_1)$ 存在 $c_1,\cdots,c_k\in C$ ($k$ 为 $(F_1^\circ)$ 中的常数) 能使

$$\Delta((\exists x)\varphi(x),\ \varphi(c_1)\vee\cdots\vee\varphi(c_k))\in T_I.$$

$(\mathrm{W}_2)$ 存在 $d_1,\cdots,d_l\in C$ ($l$ 为 $(F_2^\circ)$ 中的常数) 能使

$$\Delta((\forall x)\varphi(x),\ \varphi(d_1)\wedge\cdots\wedge\varphi(d_l))\in T_I.$$

**引理 2** 设值格 $L$ 适合 $(F_1^\circ)$ 及 $(F_2^\circ)$, 并具有弱特征式. 设 $T$ 为 $\mathcal{L}$ 中一个有限和谐的理论，$C$ 为 $\mathcal{L}$ 之外的一组新常元，其基数

$|C| = \|\mathcal{L}\|$. 令 $\overline{\mathcal{L}} = \mathcal{L} \cup C$, 则 $T$ 能扩充为 $\overline{\mathcal{L}}$ 中一个有限和谐的理论 $\overline{T}$ 使: $C$ 成为 $\overline{T}$ 在 $\overline{\mathcal{L}}$ 中的一组见证.

证明与 MT 中引理 2.1.1 者类似, 略去.

**引理 3** 设值格 $L$ 有限且具有弱特征式. 令 $T$ 为 $\mathcal{L}$ 中一个有限和谐的理论, $C$ 为 $T$ 在 $\mathcal{L}$ 中的一组见证. 则 $T$ 有一个模型 $\mathcal{U}$, 它的每一个元素都是 $C$ 中一个常元的解释.

证明见下面.

由引理 2 及 3 可得下列二定理:

**定理 1**(紧致性定理) 设值格 $L$ 有限且具有弱特征式. 令 $T$ 为 $\mathcal{L}$ 中一个有限和谐的理论, 则 $T$ 有模型.

**定理 2**(LST 定理) 设值格 $L$ 有限且具有弱特征式. 若 $\mathcal{L}$ 中的理论 $T$ 有无限模型, 则对任何基数 $\alpha \geqslant \|\mathcal{L}\|$, $T$ 都有基数为 $\alpha$ 的模型.

**引理 3 的证明** 首先由引理 1 知 $T$ 可以扩充为 $\mathcal{L}$ 中一个极大的有限和谐理论 $T_1$, 且显见 $C$ 也是 $T_1$ 在 $\mathcal{L}$ 中的一组见证. 如果我们能作出 $T_1$ 的模型, 它显然也是 $T$ 的模型. 所以, 不妨设 $T$ 自身已经是极大有限和谐的. 以下来构作 $T$ 的一个模型.

(I) 对 $C$ 中任何常元 $c, d$, 定义

$$c \sim d \quad \text{当且只当} \quad (c \equiv d) \in T_I.$$

容易证明, "$\sim$" 是 $C$ 上的等价关系.

例如, "$\sim$" 的传递性可如下证明: 设已有 $c \sim d$ 及 $d \sim e$, 则有 $(c \equiv d), (d \equiv e) \in T_I$. 今证 $(c \equiv e) \in T_I$, 从而即有 $c \sim e$. (1.1) 先证 $(c \equiv e) \in T$. 假若 $(c \equiv e) \notin T$, 则由 $T$ 的极大性知不能将 $c \equiv e$ 归入 $I$- 类而使 $T \cup \{c \equiv e\}$ 为有限和谐. 故必存在 $T$ 的有限子理论 $\Sigma$ 使 $\Sigma \cup \{c \equiv e\}$ 无有使 $c \equiv e$ 取值 $I$ 的模型. 考虑 $T$ 的有限子理论 $\Sigma \cup \{c \equiv d, d \equiv e\}$, 它有模型 (因 $T$ 为有限和谐), 取一为 $\mathcal{B}$, 则 $c \equiv d$ 与 $d \equiv e$ 在 $\mathcal{B}$ 上值均为 $I$ (因 $c \equiv d, d \equiv e \in T_I$), 从而易

见 $c \equiv e$ 在 $\mathcal{B}$ 上值为 $I$. 但 $\mathcal{B}$ 为 $\Sigma$ 的模型，这与 $\Sigma$ 的取法矛盾. 所以 $(c \equiv e) \in T$. (1.2) 设 $(c \equiv e) \in T_\lambda$, 现在证 $\lambda = I$. 考虑 $T$ 的有限子理论 $\{c \equiv d, d \equiv e, c \equiv e\}$, 取其一模型 $\mathcal{D}$. 在 $\mathcal{D}$ 上, $c \equiv d$ 与 $d \equiv e$ 值均为 $I$, 故易见 $c \equiv e$ 值也为 $I$. 但由 $c \equiv e \in T_\lambda$ 知在 $\mathcal{D}$ 上 $c \equiv e$ 值应为 $\lambda$. 所以 $\lambda = I$. (类似这样的证明，以下常常略去.)

(II) 对每一 $c \in C$, 令 $\widetilde{c}$ 为 $c$ 所在的等价类，即 $\widetilde{c} = \{d \in C : d \sim c\}$. 再令

$$A = \{\widetilde{c}: \ c \in C\}.$$

以下要在集合 $A$ 上定义与 $\mathcal{L}$ 中符号相对应的关系、常量及函数，使它成为 $T$ 的一个模型 $\mathcal{U}$.

(2.1) 对于 $\mathcal{L}$ 中任一关系符号 $P$, 我们先在 $C$ 上定义一 $n$ 元关系 $R'$ 如下：对任何 $c_1, \cdots, c_n \in C$,

$$R'(c_1 \cdots c_n) = \lambda (\neq O) \quad \text{当且只当} \quad P(c_1 \cdots c_n) \in T_\lambda.$$

(由此可知，对于 $P(c_1 \cdots c_n) \notin T$ 者，必有 $R'(c_1 \cdots c_n) = O$.) 由于 $T$ 为极大有限和谐，可以证明：若 $R'(c_1 \cdots c_n) = \lambda$ 且 $c_1 \sim d_1, \cdots, c_n \sim d_n$, 则有 $R'(d_1, \cdots, d_n) = \lambda$ (证略). 由此可知，可以合理地在 $A$ 中定义一关系 $R$ 如下：对任何 $\widetilde{c}_1, \cdots, \widetilde{c}_n \in A$,

$$R(\widetilde{c}_1 \cdots \widetilde{c}_n) = \lambda (\neq O) \quad \text{当且只当} \quad P(c_1 \cdots c_n) \in T_\lambda.$$

我们就以此关系 $R$ 作为 $P$ 在 $\mathcal{U}$ 中的解释.

(2.2) 对于 $\mathcal{L}$ 中任一常元 $d$, 考虑语句 $\varphi = (\exists v_0)(d \equiv v_0)$. 可以证明

$$\varphi \in T_1. \tag{1}$$

(证略). 另外，由 $C$ 为 $T$ 的见证可知存在 $e_1, \cdots, e_k \in C$ 能使

$$\Delta(\varphi, (d \equiv e_1) \vee \cdots \vee (d \equiv e_k)) \in T_I. \tag{2}$$

由 (1),(2) 及 $T$ 为有限和谐并注意每个 $d \equiv e_i$ 为 2 值语句，可以证明：至少有一个 $e_i$ $(1 \leqslant i \leqslant k)$ 能使 $(d \equiv e_i) \in T_I$ (证略). 这样的 $e_i$ 未必唯一，但易证 $\widetilde{e}_i$ 是唯一的. 我们就以此 $\widetilde{e}_i$ 作为 $d$ 在 $\mathcal{U}$ 中的解释. (特可知，若 $c \in C$, 则它在 $\mathcal{U}$ 中的解释是 $\widetilde{c}$.)

(2.3) 对于 $\mathcal{L}$ 中任一 $m$ 元函数符号 $F$ 及任一组 $c_1 \cdots c_m \in C$, 考虑语句 $\varphi = (\exists v_0)(F(c_1 \cdots c_m) \equiv v_0)$. 可以证明：$\varphi \in T_I$. 另外，由 $C$ 为 $T$ 的见证可知存在 $e_1 \cdots e_k \in C$ 能使

$$\Delta(\varphi, (F(c_1 \cdots c_m) \equiv e_1) \vee \cdots \vee (F(c_1 \cdots c_m) \equiv e_k)) \in T_I.$$

由此可证，在 $F(c_1 \cdots c_m) \equiv e_1, \cdots, F(c_1 \cdots c_m) \equiv e_k$ 中至少有一个在 $T_I$ 中. 此外还可证明：若有 $(F(c_1 \cdots c_m) \equiv e_i) \in T_I$ 及 $(F(c_1 \cdots c_m) \equiv e_j) \in T_I$, 则也有 $(e_i \equiv e_j) \in T_I$, 从而有 $\widetilde{e}_i = \widetilde{e}_j$. 不妨设 $(F(c_1 \cdots c_m) \equiv e_1) \in T_I$. 进一步还可证明：对于 $C$ 中的任何 $d_1, \cdots, d_m$ 及 $f_1$, 若有 $(c_1 \equiv d_1), \cdots, (c_m \equiv d_m), (e_1 \equiv f_1) \in T_I$, 则也有 $(F(d_1 \cdots d_m) \equiv f_1) \in T_I$. 由此可知，可以合理地在 $A$ 上定义一函数 $G$ 如下：对任何 $\widetilde{c}_1, \cdots, \widetilde{c}_m, \widetilde{c} \in A$,

$$G(\widetilde{c}_1 \cdots \widetilde{c}_m) = \widetilde{c} \quad \text{当且只当} \quad (F(c_1 \cdots c_m) \equiv c) \in T_I.$$

我们就以此 $G$ 作为 $F$ 在 $\mathcal{U}$ 中的解释.

模型 $\mathcal{U}$ 的定义至此完成. 以下逐步证明，$\mathcal{U}$ 是理论 $T$ 的一个模型.

(III) 首先证明，对于 $\mathcal{L}$ 中每一个无变元的项 $t$ 及每一个常元 $c \in C$：$t \equiv c$ 在 $\mathcal{U}$ 上值为 $I$ 当且只当 $(t \equiv c) \in T_I$. (3)

(3.1) 当 $t$ 为 $F(d_1 \cdots d_m)$ 形状 ($d_1, \cdots, d_m$ 为常元，未必在 $C$ 中) 时，利用 (2.3) 易证 (3) 为真.

(3.2) 当 $t$ 为 $F(t_1 \cdots t_m)$ 而 $t_1 = G_1(\cdots), \cdots, t_m = G_m(\cdots)$ 时. 设 (3) 对于 $t_1, \cdots, t_m$ 都已成立.

设 $t_1,\cdots,t_m$ 在 $\mathcal{U}$ 上的值各为 $\widetilde{e}_1,\cdots,\widetilde{e}_m$. 则易见 $t_1\equiv e_1,\cdots,$ $t_m\equiv e_m$ 在 $\mathcal{U}$ 上值均为 $I$, 故由归纳假设有

$$(t_1\equiv e_1),\cdots,(t_m\equiv e_m)\in T_I. \tag{4}$$

(3.2.1) 若 $\varphi=(F(t_1\cdots t_m)\equiv c)$ 在 $\mathcal{U}$ 上值 $I$, 则易知 $F(e_1\cdots e_m)$ $\equiv c$ 也在 $\mathcal{U}$ 上值 $I$, 故由 (3.1) 知

$$(F(e_1\cdots e_m)\equiv c)\in T_I. \tag{5}$$

假若 $(F(t_1\cdots t_m)\equiv c)\notin T$, 则由 $T$ 为极大有限和谐可知存在 $T$ 的有限子理论 $\Sigma_1$ 使

$$\Sigma_1\cup\{\varphi\}\text{无有使 }\varphi\text{ 取值 }I\text{ 的模型}. \tag{6}$$

今取 $T$ 的有限子理论 $\Sigma_1\cup\{t_1\equiv e_1,\cdots,t_m\equiv e_m,F(e_1\cdots e_m)\equiv c\}$ 的一个模型 $\mathcal{B}_1$, 由 (4) 、 (5) 知在 $\mathcal{B}_1$ 上 $t_1\equiv e_1,\cdots,t_m\equiv e_m$ 及 $F(e_1,\cdots,e_m)\equiv c$ 值均为 $I$, 从而显见 $F(t_1\cdots t_m)\equiv c$ 在 $\mathcal{B}_1$ 上值为 $I$, 与 (6) 矛盾. 所以 $(F(t_1\cdots t_m)\equiv c)\in T$. 再由 $F(t_1\cdots t_m)\equiv c$ 的 2 值性可知其在 $T_I$ 中.

(3.2.2) 若 $F(t_1\cdots t_m)\equiv c$ 在 $\mathcal{U}$ 上值 $\neq I$, 则其值为 $O$. 从而易知 $\rho=(F(e_1\cdots e_m)\equiv c)$ 也在 $\mathcal{U}$ 上值 $O$. 故由 (3.1) 知 $(F(e_1\cdots e_m)\equiv c)\notin T_I$, 再由其 2 值性可知 $(F(e_1\cdots e_m)\equiv c)\notin T$. 故可知存在 $T$ 的有限子理论 $\Sigma_2$ 使

$$\Sigma_2\cup\{\rho\}\text{无有使 }\rho\text{ 取值 }I\text{ 的模型}. \tag{7}$$

假若 $\varphi=(F(t_1\cdots t_m)\equiv c)\in T_I$, 则 $T$ 的有限子理论 $\Sigma_2\cup\{t_1\equiv e_1,\cdots,t_m\equiv e_m,\varphi\}$ 有模型 $\mathcal{B}_2$. 在 $\mathcal{B}_2$ 上, $t_1\equiv e_1,\cdots,t_m\equiv e_m$ 及 $\varphi$ 的值均为 $I$, 从而显见 $\rho$ 在 $\mathcal{B}_2$ 上的值也是 $I$, 与 (7) 矛盾. 所以 $(F(t_1\cdots t_m)\equiv c)\notin T_I$.

(IV) 由 (III) 又可得：对 $\mathcal{L}$ 中任二无变元的项 $t_1,t_2$ 都有：$t_1\equiv t_2$ 在 $\mathcal{U}$ 上值 $I$ 当且只当 $(t_1\equiv t_2)\in T_I$. (证法与 (III) 类似，略去.)

(V) 对 $\mathcal{L}$ 中任一形如 $P(t_1\cdots t_n)$ 的原子语句，都有：$P(t_1\cdots t_n)$ 在 $\mathcal{U}$ 上值 $\lambda\neq 0$ 当且只当 $P(t_1\cdots t_n)\in T_\lambda$.

证明如下：设 $t_1,\cdots,t_n$ 在 $\mathcal{U}$ 上的值各为 $\widetilde{d}_1,\cdots,\widetilde{d}_n$. 则 $t_1\equiv d_1,\cdots,t_n\equiv d_n$ 在 $\mathcal{U}$ 上值均为 $I$, 由 (III) 知 $(t_1\equiv d_1),\cdots,(t_n\equiv d_n)\in T_I$.

(5.1) 若 $P(t_1\cdots t_n)$ 在 $\mathcal{U}$ 上值 $\lambda\neq O$. 则易见 $P(d_1\cdots d_n)$ 在 $\mathcal{U}$ 上值也为 $\lambda$, 故由 (2.1) 可知 $P(d_1\cdots d_n)\in T_\lambda$. 以下证 $P(t_1\cdots t_n)\in T_\lambda$.

假若 $P(t_1\cdots t_n)\notin T$, 则由 $T$ 为极大有限和谐知存在 $T$ 的有限子理论 $\Sigma_3$ 能使 $\Sigma_3\cup\{P(t_1\cdots t_n)\}$ 无有使 $P(t_1\cdots t_n)$ 取值 $\lambda$ 的模型. 今取 $T$ 的有限子理论 $\Sigma_3\cup\{t_1\equiv d_1,\cdots,t_n\equiv d_n,P(d_1\cdots d_n)\}$ 的一个模型 $\mathcal{B}_3$, 则在 $\mathcal{B}_3$ 上 $t_1\equiv d_1,\cdots,t_n\equiv d_n$ 值均为 $I$ 而 $P(d_1\cdots d_n)$ 值为 $\lambda$, 从而显见 $P(t_1\cdots t_n)$ 值为 $\lambda$, 这与 $\Sigma_3$ 的取法矛盾. 所以 $P(t_1\cdots t_n)\in T$. 设 $P(t_1\cdots t_n)\in T_\mu$, 再证 $\mu=\lambda$:

取 $T$ 的有限子理论 $\{t_1\equiv d_1,\cdots t_n\equiv d_n,P(d_1\cdots d_n),P(t_1\cdots t_n)\}$ 的一个模型 $\mathcal{D}_1$, 则在 $\mathcal{D}_1$ 上 $t_1\equiv d_1,\cdots t_n\equiv d_n$ 值为 $I$ 而 $P(d_1\cdots d_n)$ 值为 $\lambda$, 从而 $P(t_1\cdots t_n)$ 在 $\mathcal{D}_1$ 上值也为 $\lambda$. 但由 $P(t_1\cdots t_n)\in T_\mu$ 知其在 $\mathcal{D}_1$ 上值应为 $\mu$, 所以 $\mu=\lambda$. 于是得 $P(t_1\cdots t_n)\in T_\lambda$.

(5.2) 若 $P(t_1\cdots t_n)$ 在 $\mathcal{U}$ 上值为 $O$. 以下证 $P(t_1\cdots t_n)\notin T$.

假若 $P(t_1\cdots t_n)\in T$. 设它在 $T_\nu$ 中 $(\nu\neq O)$. 因 $t_1,\cdots,t_n$ 在 $\mathcal{U}$ 上值各为 $\widetilde{d}_1,\cdots,\widetilde{d}_n$, 故知 $P(d_1\cdots d_n)$ 在 $\mathcal{U}$ 上值 $O$, 从而由 (2.1) 知 $P(d_1\cdots d_n)\notin T$. 由此可知，存在 $T$ 的有限子理论 $\Sigma_4$ 能使 $\Sigma_4\cup\{P(d_1\cdots d_n)\}$ 无有使 $P(d_1\cdots d_n)$ 取值 $\nu$ 的模型. 今取 $T$ 的有限子理论 $\Sigma_4\cup\{t_1\equiv d_1,\cdots t_n\equiv d_n,P(t_1\cdots t_n)\}$ 的一个模型 $\mathcal{B}_4$, 则在 $\mathcal{B}_4$ 上 $t_1\equiv d_1,\cdots t_n\equiv d_n$ 的值均为 $I$ 而 $P(t_1\cdots t_n)$ 值为 $\nu$, 从而

$P(d_1\cdots d_n)$ 也应值 $\nu$, 这与 $\Sigma_4$ 的取法矛盾. 所以 $P(t_1\cdots t_n)\notin T$.

下列的 (VI) 是本引理的主要结论:

(VI) 对 $\mathcal{L}$ 中每一语句 $\varphi$ 都有: $\varphi$ 在 $\mathcal{U}$ 上值 $\lambda\neq O$ 当且只当 $\varphi\in T_\lambda$.

当 $\varphi$ 为原子语句时, 由 (IV) 及 (V) 知 (VI) 为真. 以下按 $\varphi$ 的结构进行归纳来证明 (VI).

(6.1) 设 (VI) 对于 $\psi$ 已真, 则 (VI) 对于 $\varphi=\neg\psi$ 也真. 证明如下:

(6.1.1) 若 $\psi$ 在 $\mathcal{U}$ 上值 $\mu_1\neq O$. 则由归纳假设知 $\psi\in T_{\mu_1}$, 且 $\varphi$ 在 $\mathcal{U}$ 上值为 $\mu_2=\mu_1'$.

(6.1.1.1) 若 $\mu_2\neq O$, 则可证 $\varphi\in T_{\mu_2}$. (证略)

(6.1.1.2) 若 $\mu_2=O$, 今证 $\varphi\notin T$. 这是因为, 假若 $\varphi\in T$, 设 $\varphi\in T_\nu$ $(\nu\neq O)$. 取 $T$ 的有限子理论 $\{\psi,\varphi\}$ 的一个模型 $\mathcal{D}_2$. 由 $\psi\in T_{\mu_1}$ 知在 $\mathcal{D}_2$ 上 $\psi$ 值为 $\mu_1$, 从而 $\varphi$ 值为 $\mu_1'=\mu_2=O$. 但由 $\varphi\in T_\nu$ 又知在 $\mathcal{D}_2$ 上 $\varphi$ 的值应为 $\nu\neq O$, 与上矛盾. 所以 $\varphi\notin T$.

(6.1.2) 若 $\psi$ 在 $\mathcal{U}$ 上值 $\mu_1=O$. 则由归纳假设知 $\psi\notin T$, 且 $\varphi$ 在 $\mathcal{U}$ 上值为 $\mu_1'=I$. 以下证 $\varphi\in T_I$.

(6.1.2.1) 先证 $\varphi\in T$.

由 $\psi\notin T$ 及 $T$ 为极大有限和谐可知存在 $T$ 的诸有限子理论 $\Omega_1,\cdots,\Omega_u$ (设值格 $L=\{O,\lambda_1,\cdots,\lambda_u\}$, $u$ 有限.) 能使 $\Omega_i\cup\{\psi\}$ 无有使 $\psi$ 取值 $\lambda_i$ 的模型 $(i=1,\cdots,u)$.

假若 $\varphi\notin T$, 仿上又知存在 $T$ 的有限子理论 $\Omega_1'$ 能使 $\Omega_1'\cup\{\varphi\}$ 无有使 $\varphi$ 取值 $I$ 的模型. 今取 $T$ 的有限子理论 $\Omega_1\cup\cdots\cup\Omega_u\cup\Omega_1'$ 的一个模型 $\mathcal{D}_3$, 且不妨已适当膨胀得使 $\psi$ 在 $\mathcal{D}_3$ 上有值. 由诸 $\Omega_i$ 取法可知在 $\mathcal{D}_3$ 上 $\psi$ 的值为 $O$, 从而 $\varphi$ 值为 $O'=I$, 这与 $\Omega_1'$ 的取法矛盾. 所以 $\varphi\in T$. 设 $\varphi\in T_\alpha$.

(6.1.2.2) 再证 $\varphi\in T_I$.

取 $T$ 的有限子理论 $\Omega_1\cup\cdots\cup\Omega_u\cup\{\varphi\}$ 的模型 $\mathcal{D}_4$. 由诸 $\Omega_i$ 取

法可知在 $\mathcal{D}_4$ 上 $\psi$ 值为 $O$, 从而 $\varphi$ 值为 $O' = I$. 又由 $\varphi \in T_\alpha$ 知在 $\mathcal{D}_4$ 上 $\varphi$ 值应为 $\alpha$. 所以 $\alpha = I$, 即得 $\varphi \in T_I$.

(6.2) 设 (VI) 对于 $\varphi_1$ 及 $\varphi_2$ 都已真, 则 (VI) 对于 $\varphi = \varphi_1 \wedge \varphi_2$ 以及 $\varphi = \varphi_1 \vee \varphi_2$ 也真. (证仿 (6.1), 略去.)

(6.3) 设 (VI) 对于诸 $\psi(c)$ ($c$ 通过 $C$) 都已真, 则 (VI) 对于 $\varphi = (\exists x)\psi(x)$ 也真. 证明如下:

设 $\varphi$ 在 $\mathcal{U}$ 上值为 $\lambda^*$, 则 $\lambda^* = \sup\limits_{\widetilde{c} \in A} \psi(\widetilde{c})$. (此处 $\psi(\widetilde{c})$ 表示 $\psi(c)|_{\mathcal{U}}$, 以下仿此.) 再由 $L$ 适合 $(F_1^\circ)$ 知存在 $\widetilde{c}_1, \cdots, \widetilde{c}_k \in A$ 能使 $\psi(\widetilde{c}_1) \cup \cdots \cup \psi(\widetilde{c}_k) = \lambda^*$. 把 $\psi(\widetilde{c}_1), \cdots, \psi(\widetilde{c}_k)$ 各记为 $\rho_1, \cdots, \rho_k$, 则有

$$\rho_1 \cup \cdots \cup \rho_k = \lambda^*. \tag{8}$$

(6.3.1) 当 $\lambda^* \neq O$ 时. 由 (8) 知 $\rho_1, \cdots, \rho_k$ 不全为 $O$. 不妨设 $\rho_1, \cdots, \rho_r \neq O$; $\rho_{r+1} = \cdots = \rho_k = O$. $(1 \leqslant r \leqslant k)$. 故有

$$\rho_1 \cup \cdots \cup \rho_r = \lambda^*. \tag{9}$$

由归纳假设可知

$$\psi(c_1) \in T_{\rho_1}, \cdots, \psi(c_r) \in T_{\rho_r}; \quad 而 \psi(c_{r+1}), \cdots, \psi(c_k) \notin T. \tag{10}$$

又由 $T$ 有见证集 $C$ 可知存在 $d_1, \cdots, d_k \in C$ 能使

$$\Delta((\exists x)\psi(x), \psi(d_1) \vee \cdots \vee \psi(d_k)) \in T_I. \tag{11}$$

设 $\psi(d_1), \cdots, \psi(d_k)$ 在 $\mathcal{U}$ 上的值各为 $\mu_1, \cdots, \mu_k$. 不妨设其中

$$\mu_1, \cdots, \mu_h \neq O \quad 而 \ \mu_{h+1} = \cdots = \mu_k = O. \tag{12}$$

(6.3.1.1) 当 $h > 0$ 时. 由归纳假设知

$$\psi(d_1) \in T_{\mu_1}, \cdots, \psi(d_h) \in T_{\mu_h}; \quad 而 \ \psi(d_{h+1}), \cdots, \psi(d_k) \notin T. \tag{13}$$

(6.3.1.1.1) 先证 $\varphi \in T$:

假若 $\varphi \notin T$, 则存在 $T$ 的诸有限子理论 $\Sigma'_1, \cdots, \Sigma'_u$ 能使 $\Sigma'_i \cup \{\varphi\}$ 无有使 $\varphi$ 取值 $\lambda_i$ 的模型 $(i = 1, \cdots, u)$. 今取 $T$ 的有限子理论 $\Sigma'_1 \cup \cdots \cup \Sigma'_u \cup \{\psi(d_1), \cdots, \psi(d_h)\}$ 的一个模型 $\mathcal{B}_5$, (不妨设 $\mathcal{B}_5$ 已经过必要的膨胀, 使 $\varphi$ 在其上有值.) 由 (13) 知在 $\mathcal{B}_5$ 上 $\psi(d_1)$ 值 $\mu_1 > O$. 故知 $\varphi = (\exists x)\psi(x)$ 在 $\mathcal{B}_5$ 上的值 $\lambda_j = \sup\limits_{b \in B} \psi(b) \geqslant \mu_1 > O$, (其中 $B$ 是 $\mathcal{B}_5$ 的论域). 从而 $\mathcal{B}_5$ 是 $\Sigma'_j \cup \{\varphi\}$ 的使 $\varphi$ 取值 $\lambda_j (\neq O)$ 的模型, 这与 $\Sigma'_j$ 的取法矛盾. 所以 $\varphi \in T$. 设

$$\varphi \in T_\beta. \tag{14}$$

(6.3.1.1.2) 再证 $\varphi \in T_{\lambda^*}$.

由 $\psi(d_{h+1}), \cdots, \psi(d_k) \notin T$ 可知存在 $T$ 的诸有限子理论 $\Omega''_{h+1,1}, \cdots, \Omega''_{h+1,u}; \cdots; \Omega''_{k,1}, \cdots, \Omega''_{k,u}$ 能使 $\Omega''_{i,j} \cup \{\psi(d_i)\}$ 无有使 $\psi(d_i)$ 取值 $\lambda_j$ 的模型 $(i = h+1, \cdots, k; j = 1, \cdots, u)$. 今取 $T$ 的有限子理论 $\Omega''_{h+1,1} \cup \cdots \cup \Omega''_{h+1,u} \cup \cdots \cup \Omega''_{k,1} \cup \cdots \cup \Omega''_{k,u} \cup \{\psi(c_1), \cdots, \psi(c_r), \psi(d_1), \cdots, \psi(d_h), \varphi, \Delta(\varphi, \psi(d_1) \vee \cdots \vee \psi(d_k))\}$ 的一个模型 $\mathcal{D}_5$. 在 $\mathcal{D}_5$ 上, 由诸 $\Omega''_{i,j}$ 取法可知 $\psi(d_{h+1}), \cdots, \psi(d_k)$ 的值均为 $O$. 由 (13) 知 $\psi(d_1), \cdots, \psi(d_h)$ 值各为 $\mu_1, \cdots, \mu_h$. 由 (11) 知 $\Delta(\cdots)$ 值为 $I$. 由 (14) 知 $\varphi$ 值为 $\beta$. 再由 $\Delta$ 的性质知应有 $\beta = \mu_1 \cup \cdots \cup \mu_h \cup O \cup \cdots \cup O$. 又由 (10) 知在 $\mathcal{D}_5$ 上 $\psi(c_1), \cdots, \psi(c_r)$ 值各为 $\rho_1, \cdots, \rho_r$, 故应有

$$\beta = \sup_{d \in D} \psi(d) \geqslant \rho_1 \cup \cdots \cup \rho_r = \lambda^*. \tag{15}$$

(其中 $D$ 为 $\mathcal{D}_5$ 的论域). 又由 (12) 可知

$$\lambda^* = \sup_{a \in A} \psi(a) \geqslant \mu_1 \cup \cdots \cup \mu_h = \beta. \tag{16}$$

由 (15) 及 (16) 知 $\beta = \lambda^*$. 再由 (14) 即得 $\varphi \in T_{\lambda^*}$.

(6.3.1.2) 当 $h=0$ 时，仿 (6.3.1.1.2) 取 $\Omega''_{1,1},\cdots,\Omega''_{1,u};\cdots;\Omega''_{k,1},\cdots,\Omega''_{k,u}$. 再取 $T$ 的有限子理论 $\Omega''_{1,1}\cup\cdots\cup\Omega''_{1,u}\cup\cdots\cup\Omega''_{k,1}\cup\cdots\cup\Omega''_{k,u}\cup\{\psi(c_1),\cdots,\psi(c_r),\Delta(\varphi,\psi(d_1)\vee\cdots\vee\psi(d_k))\}$ 的一个模型 $\mathcal{B}_6$. 在 $\mathcal{B}_6$ 上，由诸 $\Omega''_{i,j}$ 取法可知 $\psi(d_1),\cdots,\psi(d_k)$ 的值均为 $O$. 由 (11) 知 $\Delta(\cdots)$ 值为 $I$, 再由 $\Delta$ 的性质知

$$\varphi\text{值}=O\cup O\cdots\cup O=O. \tag{17}$$

但由 (10) 知 $\psi(c_1)$ 值为 $\rho_1>O$, 故又应有 $\varphi$ 值 $=\sup\limits_{b\in B}\psi(b)\geqslant\rho_1>O$, (其中 $B$ 为 $\mathcal{B}_6$ 的论域). 这与 (17) 矛盾. 所以此情况 (6.3.1.2) 不可能出现.

(6.3.2) 当 $\lambda^*=O$ 时，以下证明 $\varphi\notin T$.

由 (9) 知 $\rho_1=\cdots=\rho_k=O$. 由 $T$ 有见证集 $C$ 知存在 $d_1,\cdots,d_k\in C$ 能使

$$\Delta((\exists x)\psi(x),\psi(d_1)\vee\cdots\vee\psi(d_k))\in T_I. \tag{18}$$

设 $\psi(d_1),\cdots,\psi(d_k)$ 在 $\mathcal{U}$ 上的值各为 $\mu_1,\cdots,\mu_k$. 则由 $O=\lambda^*\geqslant\mu_1,\cdots,\mu_k$ 知 $\mu_1=\cdots=\mu_k=O$. 故由归纳假设有 $\psi(d_1),\cdots,\psi(d_k)\notin T$. 从而存在 $T$ 的诸有限子理论 $\Omega''_{i,j}$ 能使 $\Omega''_{i,j}\cup\{\psi(d_i)\}$ 无有使 $\psi(d_i)$ 取值 $\lambda_j$ 的模型 $(i=1,\cdots,k;j=1,\cdots,u)$. 假若 $\varphi\in T$, 设 $\varphi\in T_\gamma$ $(\gamma\neq O)$. 今取 $T$ 的有限子理论 $\Omega''_{1,1}\cup\cdots\cup\Omega''_{1,u}\cup\cdots\cup\Omega''_{k,1}\cup\cdots\cup\Omega''_{k,u}\cup\{\varphi,\Delta(\varphi,\psi(d_1)\vee\cdots\vee\psi(d_k))\}$ 的一个模型 $\mathcal{D}_6$. 由诸 $\Omega''_{i,j}$ 取法知在 $\mathcal{D}_6$ 上 $\psi(d_1),\cdots,\psi(d_k)$ 的值均应为 $O$. 由 (18) 知在 $\mathcal{D}_6$ 上 $\Delta(\cdots)$ 值为 $I$, 故由 $\Delta$ 的性质知 $\varphi$ 在 $\mathcal{D}_6$ 上的值应为 $O\cup\cdots\cup O=O$. 但由 $\varphi\in T_\gamma$ 知 $\varphi$ 在 $\mathcal{D}_6$ 上的值又应为 $\gamma\neq O$, 与上矛盾. 所以 $\varphi\notin T$.

(6.4) 设 (VI) 对于诸 $\psi(c)$ ($c$ 通过 $C$) 都已真，则 (VI) 对于 $\varphi=(\forall x)\psi(x)$ 也真.

证明仿 (6.3), 略去.　　　(证毕)

## 参考文献


1 Chang C C, Keisler H J. Model Theory. Amsterdam: North-Holland Publ. Co., 1973

2 王世强. 格值模型论中紧致性定理的一种证法. 北京师范大学学报, 1980(3~4), 25~30

3 王世强, 卢景波. 格值模型的超积基本定理. 科学通报, 1981, 26: 71~74

# 第 12 章

## 变量集合与 graphs[1]

在经典集合论中，元素与元素的归属关系是最基本的关系. 1 是一个元素的集合，$X$ 为任一常量集合. 1 到 $X$ 的一个映射 $x\colon 1 \longrightarrow X$ 称为 $X$ 的一个元素，记为 $x \in X$. $X$ 的一个子集合 $A$ 定义为 $x \in A \Longrightarrow x \in X$. 两个集合 $X, Y$ 相等，定义为 $x \in X$ 当且仅当 $x \in Y$. 一个集合完全由它的元素决定.

一个常量的集合是一个装着一堆点子没有一定形状的袋子. 它的元素之间没有内聚性，是离散的. 集合的大小取决于元素的多少. 唯一可以区别两个集合的是它们包含元素的多少 (cardinality).

在离散的集合上加某种内聚性，构成不同的数学结构. 代数结构，如群、向量空间、环、域、代数等; 几何分析结构如拓扑、度量、可测、范数 (norm); 或更综合的结构，如希尔伯特空间、拓扑流形、微分流形、复盖空间，等等. 人们习惯于用集合论的语言、逻辑去讨论有关数学结构的问题.

Lawvere 等人认为可以把具有内聚性的集合，即变量的集合作为直接的学习、研究、应用对象，而不必还原到离散集合，再加上

[1]这里 graph 一词并不是专指图论，而是有更直观广泛的意义. 所以这里不将 graph 译为图论.

某种数学结构. 把变量的集合当作一般化了的集合, 可以直接运用常量集合论的语言、逻辑去讨论有关数学问题.

在变量集合的范畴中, 一个变量集合 $X$ 并不只是它的原子: $1 \longrightarrow X$ 的堆积. $X$ 由不同形状的部分构成. 例如 simplicial set 由细胞 (cell) 构成. 我们称以 $X$ 为 codomain 的一个映射 $U \longrightarrow X$ 为 $X$ 的一个一般元素 (generalized element). $X$ 由它的一般元素所决定.

在不少范畴中, 范畴的对象的一个不大的子集或类 (class) 就可以决定这一范畴中的对象.

**定义 1** $\mathcal{A}$ 是范畴 $\mathcal{E}$ 中对象的一个子集 (类), $f, g$ 是任意两个具有相同定义域以及 codomain 的映射, $f, g: X \longrightarrow Y$, 若 $f \neq g$, 那么存在 $A \in \mathcal{A}$, $x: A \longrightarrow X$, $f \circ x \neq g \circ x$, 这样称 $\mathcal{A}$ 为生成元集 (类).

例如一个元素的集合 1 即是常量集合范畴 $\mathcal{S}$ 的生成元. simplicial set 的生成元集是 $\{n\text{–cell}, n = 0, 1, 2, \cdots\}$

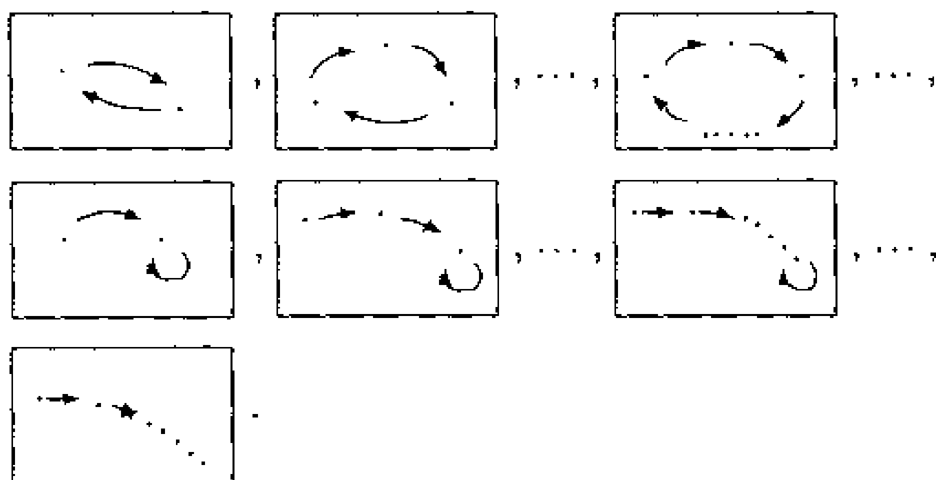
在这一章里, 我们讨论一种很简单的内聚性: graph. 首先, dynamical set 是一种 graph.

一个 dynamical set $X^{\circlearrowright t}$ 是一个集合 $X$, 以及一个自身到自身的映射, dynamic $t: X \longrightarrow X$. $t$ 把 $X$ 的每一个元素送到下一个元素. 两个 dynamical set $X^{\circlearrowright t}$ 到 $Y^{\circlearrowright s}$ 之间的映射是 $X$ 到 $Y$ 的一个映射, 并且保持 dynamic, $f: X^{\circlearrowright t} \longrightarrow Y^{\circlearrowright s}$

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle t}\downarrow & & \downarrow{\scriptstyle s} \\ X & \xrightarrow{f} & Y \end{array}$$

$ft = sf$. 记 dynamical set 以及它们之间映射的范畴为 $\mathcal{S}^{\circlearrowright}$

由一个元素的 dynamical set 1 到任一 dynamical set $X^{\circlearrowleft}$ 的一个映射是 $X^{\circlearrowleft}$ 的一个固定点. 若一个 dynamical set 不具有固定点, 那么 $X^{\circlearrowleft}$ 就不具有通常意义的元素. 所以要了解 dynamical set $X^{\circlearrowleft}$ ，只知道 $X^{\circlearrowleft}$ 的固定点是远远不够的. 我们需要了解 $X^{\circlearrowleft}$ 中的 2 cycle, 3 cycle,$\cdots$, $n$ cycle, $\cdots$, 以及其他性质. 即需要知道由以下 dynamical sets 到 $X^{\circlearrowleft}$ 的映射.

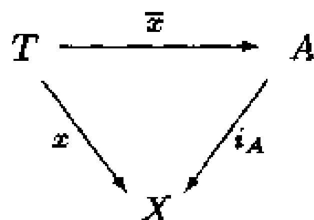


{ } 是 dynamical sets 的范畴 $S^{\circlearrowleft}$ 的一个最小生成元集.

**定义 2** $\mathcal{E}$ 是任意一个范畴, $X$ 是 $\mathcal{E}$ 中一个对象.

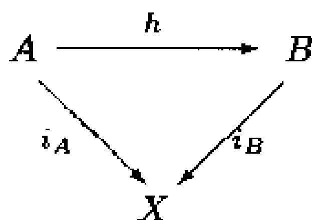
(1) $A$ 是 $X$ 的一个部分 (子对象), 若存在 $A$ 到 $X$ 的一个 monomorphism $i: A \longrightarrow X$.

(2) $x$ 是 $X$ 的一个元素, $x: T \longrightarrow X$. $A$ 是 $X$ 的一个部分. 若存在 $\overline{x}: T \longrightarrow A$, 使以下三角形可换



$i_A \circ \overline{x} = x$, 我们说 $x$ 属于 $A$, 记为 $x \in A$.

(3) $A, B$ 是 $X$ 的部分, 即有 $i_A: A \longrightarrow X$, $i_B: B \longrightarrow X$ 均为 monomorphism. 若存在 $A$ 到 $B$ 的映射 $h: A \longrightarrow B$ 使得 $i_A = i_B \circ h$. 我们记 $A \subseteq B$.




**命题 1** $A, B$ 是 $X$ 的部分. $A \subseteq B$ 当且仅当 $\forall x(x \in A \Longrightarrow x \in B)$.

**证明** 必要性. 若 $A \subseteq B$, 即存在 $h: A \longrightarrow B$, $i_A = i_B \circ h$. 对 $x \in A$, $x: T \longrightarrow X$, $\overline{x}: T \longrightarrow A$, $x = i_A \circ \overline{x}$. 让 $\overline{\overline{x}} = h \circ \overline{x}$, 那么 $i_B \circ \overline{\overline{x}} = i_B \circ h \circ \overline{x} = i_A \circ \overline{x} = x$. 这样 $x \in A \Longrightarrow x \in B$.

充分性. 若 $\forall x(x \in A \Longrightarrow x \in B)$, 特别让 $x = i_A: A \longrightarrow X$, 那么存在 $h: A \longrightarrow B$, 使得 $i_A = i_B \circ h$, 即 $A \subseteq B$.

**命题 2** 若 $A \subseteq B$, 那么 $A$ 是 $B$ 的一个部分, 即 $h: A \longrightarrow B$ 为 monomorphism.

**证明** 若有 $f, g: C \longrightarrow A$, 且 $h \circ f = h \circ g$, 因为 $i_B \circ h = i_A$, 有 $i_A \circ f = i_B \circ h \circ f = i_B \circ h \circ g = i_A \circ g$. 因为 $i_A$ 是 monomorphism, 所以有 $f = g$. 这样, $h$ 是 monomorphism.

有了元素、部分、元素从属关系的一般定义后, 我们就可以运用在常量集合的范畴 $\mathcal{S}$ 中的有关元素的逻辑语言于任一变量集合的范畴内. 这样在很大程度上就可以把变量集合作为已熟悉的常量集合来对待.

例如在 $\mathcal{S}$ 中集合 $X$ 到集合 $Y$ 的两个映射 $f, g: X \longrightarrow Y$ 的 equalizer 定义为 $E = \{x \in X \mid fx = gx\}$. 这一定义同样可以用于

任一变量集合的范畴 $\mathcal{E}$. 让 $X, Y$ 为 $\mathcal{E}$ 中对象， $f, g: X \longrightarrow Y$ 的 equalizer 是 $X$ 的一个部分 $E$, 具有性质 $f \circ i = g \circ i$, 若 $X$ 的

$$\begin{array}{ccccc} E & \overset{i}{\hookrightarrow} & X & \overset{f}{\underset{g}{\rightrightarrows}} & Y \\ {\scriptstyle h}\uparrow & \nearrow{\scriptstyle x} & & & \\ T & & & & \end{array}$$

元素 $x: T \longrightarrow X$, 满足 $fx = gx$, 那么 $x \in E$, 即存在 $h: T \longrightarrow E$, 使得 $x = i \circ h$.

常量集合范畴 $\mathcal{S}$ 是变量集合范畴的特例. 很多变量集合的范畴可以从 $\mathcal{S}$ 上构造. 例如 $\mathcal{S}$ 上的各种函子范畴. 若取 $\mathcal{C}$ 为只含一个对象以及一个恒等映射的范畴，那么函子范畴 $\mathcal{S}^{\mathcal{C}} = \mathcal{S}$. 这里我们介绍三种简单的函子范畴，它们均与 graph 有关. 这就是 dynamic sets $\mathcal{S}^{\circlearrowleft}$ , graph(irreflexive) $\mathcal{S}^{\Delta_0^{op}} = \mathcal{S}^{(\downdownarrows)^{op}}$ , 和 reflexive graph $\mathcal{S}^{\Delta^{op}}$.

我们已见过 dynamical sets $\mathcal{S}^{\circlearrowleft}$ . 实际上 $\mathcal{S}^{\circlearrowleft}$ 也是一个函子范畴. 让 $N$ 代表自然数的集合 $N = \{0, 1, 2, \cdots\}$, 且具有加法. 这样 $N$ 是有单位元的半群 (monoid). 因而 $N$ 可以看为只有一个对象的范畴. 这样，函子范畴 $\mathcal{S}^N = \mathcal{S}^{\circlearrowleft}$ 正是 dynamical sets 的范畴. 特别 $N$ 本身是一个 dynamical set, 具有 dynamic $s: N \longrightarrow N$, $s$ 一般称为 successor map, $s(n) = n + 1$. 让 $X$ 为一个 dynamical set, 具有 dynamic $t: X \longrightarrow X$. 那么， $N$ 到 $X$ 的在 $\mathcal{S}^{\circlearrowleft}$ 内的一个映射 $x: N \longrightarrow X$. 即是 $X$ 中的一个序列 $x = \{x_0, x_1, x_2, \cdots\}$, $x_0 = x(0), x_1 = t(x_0), \cdots, x_n = t^n(x_0), \cdots$. 这个序列完全由它的起始元素 $x_0$ 以及 $X$ 中的 dynamic $t$ 决定. 这样有以下的一一自然对应

$$\frac{N \longrightarrow X \qquad \text{在 } \mathcal{S}^{\circlearrowleft} \text{ 内}}{1 \longrightarrow X \qquad \text{在 } \mathcal{S} \text{ 内}}$$

这可以表示为：$X$ 是一个集合，对 $X$ 中的任一个元素 $x_0$，以及 $X$ 到 $X$ 的一个映射 $t: X \longrightarrow X$，存在 $X$ 的一个序列 $x: N \longrightarrow X$，具有性质 $x(0) = x_0$，$x(n+1) = t(x(n))$，即下面的三角形正方形可换

$$\begin{array}{ccccc} 1 & \xrightarrow{o} & N & \xrightarrow{s} & N \\ & \searrow^{x_0} & \downarrow{x} & & \downarrow{x} \\ & & X & \xrightarrow{t} & X \end{array}$$

序列 $x$ 称为以 $x_0$ 为起点的简单递归 (recursion).

**递归引理** $h: N \times A \longrightarrow A$ 为 $\mathcal{S}$ 中任一映射. 给出 $a_0: 1 \longrightarrow A$，存在 $A$ 中唯一序列 $g: N \longrightarrow A$，满足条件 $g(0) = a_0$，$g(n+1) = h(n, g(n))$.

**证明** 定义

$$t: N \times A \longrightarrow N \times A,$$
$$t(n, a) = (n+1, h(n, a)),$$
$$x_0 = (0, a_0).$$

由简单递归，存在 $N \times A$ 的唯一一个序列 $x: N \longrightarrow N \times A$，具有性质 $x(0) = (0, a_0)$，$x(n+1) = t(x(n))$.

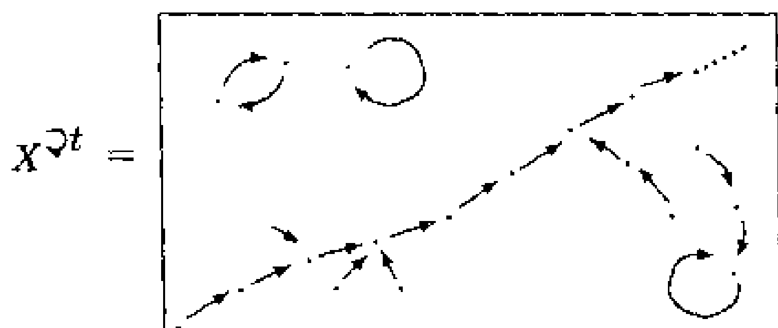
让 $P_N: N \times A \longrightarrow N$，$P_A: N \times A \longrightarrow A$ 分别为 $N \times A$ 到 $N$ 和 $A$ 的投影. 定义 $k = P_N \circ x$，$g = P_A \circ x$. 那么

$$\begin{aligned} x(n) &= (k(n), g(n)) = (n, g(n)). \\ g(0) &= P_A \circ x(0) = P_A(0, a_0) = a_0, \\ g(n+1) &= P_A \circ x(n+1) = P_A(t(x(n))) \\ &= P_A(t(n, g(n))) = P_A(n+1, h(n, g(n))) \\ &= h(n, g(n)). \end{aligned}$$

由于 $x$ 是唯一的，故 $g$ 也是唯一的.

一个 dynamical set $X^{\circlearrowleft t}$ 是如下的一个 graph: 集合 $X$ 的元素为 graph 的点子 (dot), dynamic $t$ 给出箭头的方向.

$X^{\circlearrowleft t}$ =



它的特点是，从每一个点子一定有一个，而且只有一个箭头发出. $X^{\circlearrowleft}$ 有两个有意思的子系统 (部分),

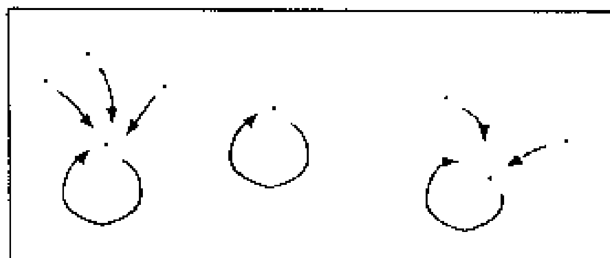
$$X_0 = \{x \in X \mid t(x) = x\},$$
$$X_\infty = \{x \in X \ : \ t^n(x) \notin X_0, \ \forall n \in N\}.$$

$X_0$ 是 dynamic $t$ 的固定点集. 而 $X_\infty$ 可称为 dynamic $t$ 的振荡点集.

我们也可以定义 $X_k = \{x \in X \mid t^k(x) \in X_0, \ t^{k-1}(x) \notin X_0\}$, $X_k$ 包含的元素距固定点有 $k$ 步. 但 $X_k$ 不是 $X^{\circlearrowleft t}$ 的子系统，因为 $t(X_k) \subseteq X_{k-1}$. 含 $\overline{X}_k = \bigcup\limits_{i \leqslant k} X_i = \{x \in X \mid t^i(x) \in X_0, i \leqslant k\}$, $\overline{X}_k$ 是 $X^{\circlearrowleft t}$ 的一个子系统.

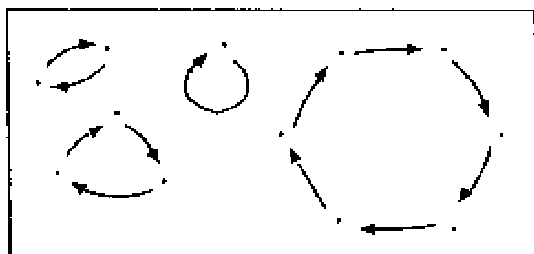
$S^{\circlearrowleft}$ 有两个子范畴，一个是 idempotents $S^C$, 另一个是 automorphisms $S^{\rightleftarrows}$ .

一个 idempotent 的图形如下：



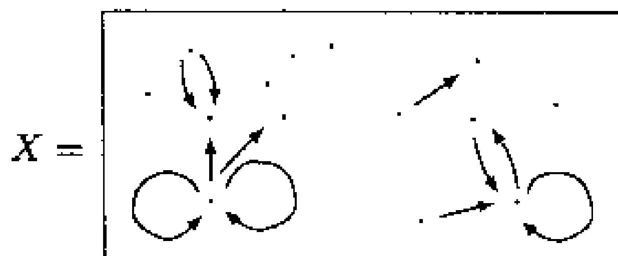
这就是说 dynamic set $X^{\circlearrowright}$ 是一个 idempotent, 如果 $X^{\circlearrowright} = X_0 \cup X_1 = \overline{X}_1$.

若 $t: X \longrightarrow X$ 是可逆的, 则称 $t$ 为一个 automorphism. 一个 dynamic 为自同构的 graph, 不包含分枝, 而只有 cycles. 如图:



$t$ 的逆映射 $t^{-1}$ 即为"倒着转".

一个一般的 graph $X$ 如下图:

$X =$ 

$X$ 具有点子和箭头. 记 $X$ 中点子的集合为 $X_0$, 箭头的集合为 $X_1$. 从 $X_1$ 到 $X_0$ 有两个映射 $d_0, d_1$,

$$X_1 \underset{d_1}{\overset{d_0}{\rightrightarrows}} X_0$$

$d_0$ 把一个箭头送到它的起点，$d_1$ 把箭头送到它的终点．可以记 $X = \left(X_1 \underset{d_1}{\overset{d_0}{\rightrightarrows}} X_0\right)$．

若 $Y = \left(Y_1 \underset{d_1}{\overset{d_0}{\rightrightarrows}} Y_0\right)$ 也是一个 graph, 那么 $X$ 到 $Y$ 的一个映射 $f: X \longrightarrow Y$, 保持 graph 的结构，即把点子送到点子，箭头送到箭头，并且是相容的 (compatible)．这就是说 $f = (f_0, f_1)$．

$$\begin{array}{ccc} X_1 & \xrightarrow{f_1} & Y_1 \\ d_0 \downarrow\downarrow d_1 & & d_0 \downarrow\downarrow d_1 \\ X_0 & \xrightarrow{f_0} & Y_0 \end{array}$$

$$f_0 \circ d_0 = d_0 \circ f_1, \qquad f_0 \circ d_1 = d_1 \circ f_1.$$

这样一般 graph 的范畴正是函子范畴 $\mathcal{S}^{\Delta_0^{op}}$, 这里 $\Delta_0$ 是范畴 $\left\{T \underset{d_1}{\overset{d_0}{\rightrightarrows}} A\right\}$, $A$ 代表 arrow, $T$ 代表 target．一个 graph $X \in \mathcal{S}^{\Delta_0^{op}}$, $X(A)$ 是箭头的集合，$X(T)$ 是点子的集合，$X(A) \underset{d_1}{\overset{d_0}{\rightrightarrows}} X(T)$．$d_0, d_1$ 给出箭头的起点和终点 (注意，这里仍记 $X(d_0), X(d_1)$ 为 $d_0, d_1$)．

特别 $A$ 和 $T$ 本身也是 graph．

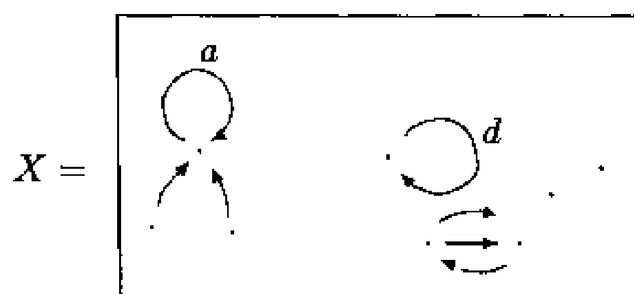
$\mathcal{S}^{\Delta_0^{op}}(A, A) = \{1_A\}$, $\mathcal{S}^{\Delta_0^{op}}(T, A) = \{d_0, d_1\}$, $A$ 本身作为 graph 含有一个箭头和两个点子．由 $\mathcal{S}^{\Delta_0^{op}}(d_0, A)$, $\mathcal{S}^{\Delta_0^{op}}(d_1, A)$ 决定箭头的起点与终点

$$\text{A} = \boxed{\overset{d_0}{\cdot} \xrightarrow{\ 1_A\ } \overset{d_1}{\cdot}}$$

$T$ 自身作为 graph 只含有一个点 $\boxed{\cdot}$．这是因为 $\mathcal{S}^{\Delta_0^{op}}(A, T) = \phi$, $\mathcal{S}^{\Delta_0^{op}}(T, T) = \{1_T\}$．

由 Yoneda 引理，对任一 graph $X$, $X(A) = \mathcal{S}^{\Delta_0^{op}}(A, X)$ 给出 $X$ 的箭头，$X(T) = \mathcal{S}^{\Delta^{op}}(T, X)$ 给出 $X$ 的点子.

Loop $\boxed{\cdot\circlearrowleft}$ 是 $\mathcal{S}^{\Delta_0^{op}}$ 中的 terminal 对象. 记 $1 = \boxed{\cdot\circlearrowleft}$ . 这样一个 graph $X$ 中的点，即 1 到 $X$ 的映射是 $X$ 中的一个 loop. 注意， graph 中的点子并不是这种意义下的 “点”. 例如




$\mathcal{S}^{\Delta_0^{op}}(1, X) = \{ \cdot\circlearrowleft^a, \cdot\circlearrowleft^d \}$. 记 $\mathcal{S}^{\Delta_0^{op}}(1, X) = \mathrm{pt}(X)$. pt 是 $\mathcal{S}^{\Delta_0^{op}}$ 到 $\mathcal{S}$ 的一个函子.

让 $B \in \mathcal{S}$, 是一常量集合. $B$ 可以看为离散的 graph, 即每一点有一个 loop. 例如 $B$ 有三个点. 那么 $\mathrm{discrete}(B) = \boxed{\cdot\circlearrowleft\ \cdot\circlearrowleft\ \cdot\circlearrowleft}$ . discrete 是由常量集合的范畴 $\mathcal{S}$ 到 $\mathcal{S}^{\Delta_0^{op}}$ 的函子.

若 $X$ 是一个 graph, 让 $\pi_0(X)$ 为 $X$ 的连通分支的集合. 这样 $\pi_0$ 是从 $\mathcal{S}^{\Delta_0^{op}}$ 到 $\mathcal{S}$ 的一个函子.

**定理 1** $\pi_0$ 是函子 discrete 的 left adjoint, discrete 是函子 pt 的 left adjoint.

这就是说，对 graph $X$, 集合 $B$, 存在以下一一自然对应：

$$\mathcal{S}(\pi_0(X), B) \approx \mathcal{S}^{\Delta_0^{op}}(X, \mathrm{discrete}(B)),$$

$$\mathcal{S}^{\Delta_0^{op}}(\mathrm{discrete}(B), X) \approx \mathcal{S}(B, \mathrm{pt}(X)).$$

这很像拓扑空间和连续映射的范畴 Top 与集合的范畴 $\mathcal{S}$ 之间的关系. $X$ 是一个拓扑空间， $B$ 是一个集合， $\mathrm{discrete}(B)$ 是在

$B$ 上加上离散拓扑，$\pi_0(X)$ 是 $X$ 的连通分支的集合，而 $\mathrm{pt}(X)$ 是 $X$ 的点的集合，那么有一一自然对应

$$\frac{\pi_0(X) \longrightarrow B \qquad \text{在 } \mathcal{S} \text{ 内}}{X \longrightarrow \mathrm{discrete}(B) \quad \text{在 Top 内}}$$

以及

$$\frac{\mathrm{discrete}(B) \longrightarrow X \qquad \text{在 Top 内}}{B \longrightarrow pt(X) \quad \text{在 } \mathcal{S} \text{ 内}}$$

graph 的范畴 $\mathcal{S}^{\Delta_0^{op}}$ 是卡氏积封闭的. 这是说若 $X, Y, Z$ 是 graph, 那么存在 graph $Z^Y$, 即 $Y$ 到 $Z$ 的函数空间, 满足一一自然对应.

$$\frac{X \times Y \longrightarrow Z}{X \longrightarrow Z^Y}$$

下面是有关 graph 函数空间的例子.

$$A = \boxed{0 \cdot \xrightarrow{a} \cdot 1}, \quad T = \boxed{\cdot 2}, \quad 1 = \boxed{\circlearrowleft}$$

我们先计算 $A^A$.

由 Yoneda 引理，$A^A$ 中的点子集 $A^A(T)$ 相应于 $T$ 到 $A^A$ 在 $\mathcal{S}^{\Delta_0^{op}}$ 中的映射：$T \longrightarrow A^A$. 而由 $\mathcal{S}^{\Delta_0^{op}}$ 的卡氏积封闭性有以下一一自然对应.

$$\frac{T \longrightarrow A^A}{T \times A \longrightarrow A}$$

$A^A$ 中的箭头集 $A^A(A)$ 相应于

$$\frac{A \longrightarrow A^A}{A\times A \longrightarrow A}$$

graph $T\times A = \boxed{\begin{matrix}\cdot\,(2,1)\\ \cdot\,(2,0)\end{matrix}}$ ,它不具有箭头,这是因为 $T\times A(A) = T(A)\times A(A) = \phi\times\{a\} = \phi$;

graph $A\times A = \boxed{\begin{matrix}(0,1) & (1,1)\\ (a,a)\nearrow & \\ (0,0) & (1,0)\end{matrix}}$

$T\times A$ 到 $A$ 的 graph 映射有 4 个, $I$,1,O,$\tau$:

$$I:\quad I(2,0)=0,\quad I(2,1)=1;$$
$$1:\quad 1(2,0)=1,\quad 1(2,1)=1;$$
$$O:\quad O(2,0)=0,\quad O(2,1)=0;$$
$$\tau:\quad \tau(2,0)=1,\quad \tau(2,1)=0.$$

$$\underset{T\times A}{\boxed{\begin{matrix}(2,1)\\ \cdot\\ \\ \cdot\\ (2,0)\end{matrix}}} \longrightarrow \underset{A}{\boxed{\begin{matrix}1\\ \uparrow\\ 0\end{matrix}}}$$

$\{I,1,O,\tau\}$ 为 $A^A$ 中的点子.

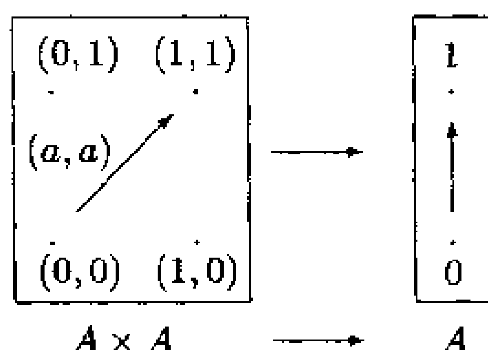
$A\times A$ 到 $A$ 的 graph 映射也是 4 个，$a_1,a_2,a_3,a_4$. graph 映射必须把点子送到点子，箭头送到箭头. 并且箭头的起点送到起点，终点送到终点.

$$a_1:\quad a_1(0,0)=a_1(1,0)=0,\ \ a_1(0,1)=a_1(1,1)=1;$$

$$a_2:\quad a_2(0,0)=a_2(0,1)=0,\ \ a_2(1,0)=a_2(1,1)=1;$$

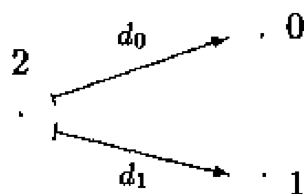
$$a_3:\quad a_3(0,0)=a_3(0,1)=a_3(1,0)=0,\ \ a_3(1,1)=1;$$

$$a_4:\quad a_4(0,0)=0,\ \ a_4(1,1)=a_4(1,0)=a_4(0,1)=1.$$




$\{a_1,a_2,a_3,a_4\}$ 是 $A^A$ 中的箭头. 箭头的起始由以下因素决定.

$$d_0,d_1:\ T\longrightarrow A$$
$$d_0(2)=0,\ d_1(2)=1,$$




$d_0\times 1_A$, $d_1\times 1_A:\ T\times A\longrightarrow A\times A$ 给出 $T\times A$ 到 $A\times A$ 的两个 graph 映射. 对 $i=1,2,3,4$, 映射的复合

$$a_i\circ(d_0\times 1_A)\ \text{给出}\ a_i\ \text{的起点,}$$

$$a_i\circ(d_1\times 1_A)\ \text{给出}\ a_i\ \text{的终点.}$$

$$
\begin{array}{ccc}
T \times A & \overset{a_i \circ (d_0 \times 1_A)}{\underset{a_i \circ (d_1 \times 1_A)}{\rightrightarrows}} & A \\
{\scriptstyle d_0 \times 1_A} \downarrow\downarrow {\scriptstyle d_1 \times 1_A} & & \\
A \times A & \xrightarrow{\quad a_i \quad} & A
\end{array}
$$

$$a_1 \circ (d_0 \times 1_A) = I, \quad a_1 \circ (d_1 \times 1_A) = I;$$

$$a_2 \circ (d_0 \times 1_A) = 0, \quad a_2 \circ (d_1 \times 1_A) = 1;$$

$$a_3 \circ (d_0 \times 1_A) = 0, \quad a_3 \circ (d_1 \times 1_A) = I;$$

$$a_4 \circ (d_0 \times 1_A) = 1, \quad a_4 \circ (d_1 \times 1_A) = I.$$

所以

$A^A =$

1 $T$ $a_4$ $a_2$ $a_1$ $I$ $a_3$ $O$

因为 1 = 是 terminal object, 所以 $A \times 1 = A$, $A^1 = A$, $1^A = 1$.

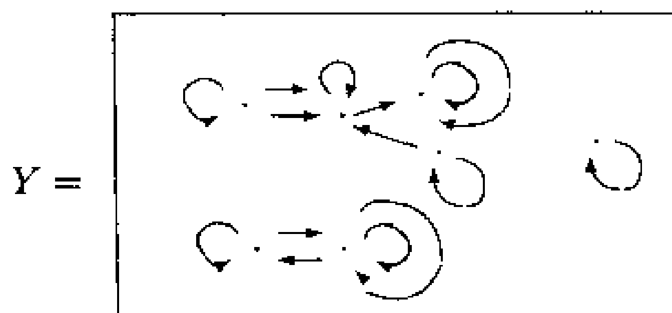
$$T \times T = , \quad T^A = ,$$
$$A \times T = .$$

$A^T$ 的点子 $A^T(T)$ 有两个, 这是因为从 $T \times T$ 到 $A$ 的映射有两个; $A^T$ 的箭头有四个, 这是因为从 $A \times T$ 到 $A$ 的映射有四个. 通过相应的计算,

$A^T =$ .

一个 dynamical set $X^{\circlearrowleft t}$ 可以看为是一个 graph, 即 graph $X \overset{d_0=1_X}{\underset{d_1=t}{\rightrightarrows}} X$.

Reflexive graph 也是一种 graph. Reflexive graph 的特点是它的每一个点子都结合有一个 loop, 如下图

$Y =$ 

这样一个 reflexive graph $Y$ 也包含有两个集合, 点子的集合 $Y_0$, 箭头的集合 $Y_1$, 以及三个映射 $d_0, d_1: Y_1 \longrightarrow Y_0, i: Y_0 \longrightarrow Y_1$, $i$ 将每一个点子映到与它相应的 loop(称为退化了的箭头), 并且满足 $d_0 \circ i = d_1 \circ i = 1_{Y_0}$.

如果我们记 $i \circ d_0 = \partial_0$, $i \circ d_1 = \partial_1$, $1_{Y_1} = 1$. 这样 $\partial_i \circ \partial_j = (i \circ d_i) \circ (i \circ d_j) = i \circ (d_i \circ i) \circ d_j = i \circ 1_{Y_0} \circ d_j = i \circ d_j = \partial_j$. $\mathbf{\Delta_1} = \{\mathbf{1}, \partial_0, \partial_1\}$ 构成一个有单位元的半群. Reflexive grahp $Y$ 又可以看成一个具有右 $\mathbf{\Delta}_1$-action 的集合.

因为是右 $\mathbf{\Delta}_1$-action, 所以我们将 $\mathbf{\Delta_1}$ 中的乘法写为 $\partial_i \circ \partial_j = \partial_j \partial_i$. 这样有 $\partial_i \partial_j = \partial_i$.

若 $X$ 是一个右 $\mathbf{\Delta_1}$-set, $X \times \mathbf{\Delta_1} \longrightarrow X$, $\mathbf{\Delta_1}$ 的元素作用在 $X$ 的元素上. 可以把 $X$ 中的元素都看为箭头, 而 $\partial_0, \partial_1$ 的作用告诉我们箭头的起点和终点. 如 $x \in X$, $x\partial_0 \overset{x}{\longrightarrow} x\partial_1$.

**定义 3** $X$ 是一个右 $\mathbf{\Delta_1}$-set. $x \in X$, 若有 $x\partial_0 = x = x\partial_1$, 我们称 $x$ 是一个退化了的 (degenerated) 箭头, 即一个点子.

对于退化了的箭头, 我们很多时候就用点子来表示, 而不必画

出退化了的箭头. 让 $X_0 = \{x \in X \mid x\partial_0 = x = x\partial_1\}$ 为 $X$ 中的点子集. 可以记 $X = X_1$, 那么 $i: X_0 \longrightarrow X_1$, $\partial_0, \partial_1: X_1 \longrightarrow X_0$.

由一个右 $\mathbf{\Delta_1}$-set 到另一个右 $\mathbf{\Delta_1}$-set 的保持 $\mathbf{\Delta_1}$-action 的映射正是 graph 映射. 所以 reflexive graph 和 graph 映射的范畴正是 $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$.

$\mathbf{\Delta_1}$ 本身是一个 reflexive graph:

$\partial_0\partial_0 = \partial_0 = \partial_0\partial_1$, $\partial_1\partial_0 = \partial_1 = \partial_1\partial_1$, 所以 $\partial_0, \partial_1$ 是两个点子, 而 $1\partial_0 = \partial_0$, $1\partial_1 = \partial_1$, 1 是一个连接 $\partial_0$ 与 $\partial_1$ 的箭头.
$\mathbf{\Delta_1} = \boxed{\partial_0 \cdot \xrightarrow{1} \cdot \partial_1}$

将一个 graph$X \in \mathcal{S}^{\mathbf{\Delta}_0^{op}}$ 中的点子都看为是退化了的箭头. 那么 $X$ 是一个 reflexive graph. 但是 $\mathcal{S}^{\mathbf{\Delta}_0^{op}}$ 中的映射与 $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 中的映射却是有区别的. $\mathcal{S}^{\mathbf{\Delta}_0^{op}}$ 中的映射必须把点子送到点子, 箭头送到箭头; 而在 $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 中的 graph 映射则把点子送到点子, 而箭头却可以送到箭头或点子 (退化了的箭头). 所以只含一个点 (退化了的箭头) 的 reflexive graph 是 $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 中的 terminal 对象, $1 = \boxed{\cdot}$.

这样在一个 reflexive graph $Y$ 中点子 (dot) 正是所谓的点 (point), 即由 1 到这个 reflexive graph 的映射. 所以点对决定一个 graph 并不起很大作用. 决定一个 reflexive graph 的是箭头, 即由 $\mathbf{\Delta_1}$ 到 $Y$ 的映射 $\mathcal{S}^{\mathbf{\Delta}_1^{op}}(\mathbf{\Delta_1}, Y)$.

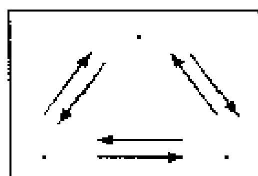
对 reflexive graph $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 也有

连通分支函子　$\pi_0: \mathcal{S}^{\mathbf{\Delta}_1^{op}} \longrightarrow \mathcal{S}$,

discrete graph 函子　discrete: $\mathcal{S} \longrightarrow \mathcal{S}^{\mathbf{\Delta}_1^{op}}$,

以及点的函子　pt: $\mathcal{S}^{\mathbf{\Delta}_1^{op}} \longrightarrow \mathcal{S}$. 并且 $\pi_0$ 是 discrete 的 left adjoint, discrete 是 pt 的 left adjoint.

对于 reflexive graph, 除了 discrete graph 函子外, 还有 codiscrete graph 函子, codiscrete: $\mathcal{S} \longrightarrow \mathcal{S}^{\mathbf{\Delta}_1^{op}}$. codiscrete graph 是一种极端连通的 graph. 它的每一点都与另外一点在两个方向上相联. 例如, 三个元素的 codiscrete graph



codiscrete graph 的极端对称有序实际上成为一种混沌 (chaos). 这是因为从中得不到任何有意思的信息.

**定理 2** 函子 pt 是函子 codiscrete 的 left adjoint. 即有一一自然对应

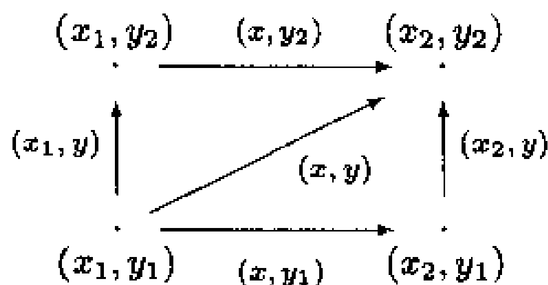
$$\frac{\mathrm{pt}(X) \longrightarrow B \qquad \text{在 } \mathcal{S} \text{ 内}}{X \longrightarrow \mathrm{codiscrete}(B) \text{ 在 } \mathcal{S}^{\Delta_1^{op}} \text{ 内}}$$

这是因为 reflexive graph $X$ 的每一个点子都是点, 而 codiscrete($B$) 是极端连通的. 这样 $X$ 到 codiscrete($B$) 的一个 graph 映射正是由 $X$ 的点子的集合到集合 $B$ 的一个任意映射. 这与 codiscrete 拓扑空间的情形一样.

Reflexive graph 范畴 $\mathcal{S}^{\Delta_1^{op}}$ 有很多很好的性质, codiscrete graph 的存在是其一, 下面便是另一个

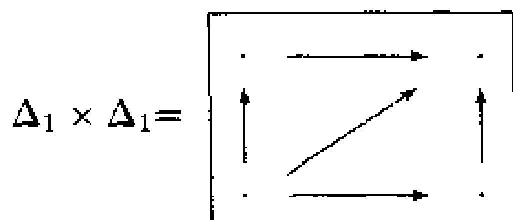
**定理 3** 连通分支函子 $\pi_0 : \mathcal{S}^{\Delta_1^{op}} \longrightarrow \mathcal{S}$ 保持乘积. 即 $\pi_0(X \times Y) \approx \pi_0(X) \times \pi_0(Y)$.

这是因为, 若 $X, Y$ 是 reflexive graph, $x_1, x_2; y_1, y_2$ 在 $X, Y$ 内分别被 $x, y$ 连接, $x\partial_0 = x_1$, $x\partial_1 = x_2$; $y\partial_0 = y_1$, $y\partial_1 = y_2$ 在乘积 $X \times Y$ 中由 $x_1, x_2, y_1, y_2$ 产生的四个点子是连接在一起的 ($x_1, x_2, y_1, y_2$ 是退化了的箭头).



而 graph 的连通分支函子 $\pi_0$ : $\mathcal{S}^{\mathbf{\Delta}_0^{op}} \longrightarrow \mathcal{S}$ 并不保持乘积. 例如, $I = \boxed{\cdot \longrightarrow \cdot}$ 有一个连通分支, 而 $I \times I = \boxed{\begin{smallmatrix} \cdot & \cdot \\ \cdot \nearrow & \cdot \end{smallmatrix}}$ 有三个连通分支.

Reflexive graph $\mathbf{\Delta}_1 = \boxed{\cdot \longrightarrow \cdot}$ 的乘积 $\mathbf{\Delta}_1 \times \mathbf{\Delta}_1$ 具有九个元素, 即九个箭头, 其中四个是退化了的. 应用 $\partial_0 \times \partial_0, \partial_1 \times \partial_1$ 于另外五个箭头, 给出它们的起点和终点.

$\Delta_1 \times \Delta_1 =$ 

常量集合的范畴 $\mathcal{S}$ 具有真值对象 $\Omega$(truth value object), $\Omega$ 又称为 subobject classifier. 在 $\mathcal{S}$ 中 $\Omega$ 是两个元素的集合 $\Omega = 2 = \{t, f\}$, $t$ 代表真 (true), $f$ 代表假 (false). $X$ 是一个集合, $X$ 的一个子集 $A$ 对应于一个从 $X$ 到 $\Omega$ 的映射

$$\varphi_A : X \longrightarrow \Omega, \quad \varphi_A(x) = \begin{cases} t, & 若\ x \in A \\ f, & 若\ x \notin A. \end{cases}$$

这就是说, 下面的图形是一个 pullback 图形

$$\begin{array}{ccc} A & \hookrightarrow & X \\ \downarrow & & \downarrow{\scriptstyle \varphi_A} \\ 1 & \xrightarrow{t} & \Omega \end{array}$$

这样, 集合 $X$ 的子集一一对应于 $X$ 到 $\Omega$ 的映射, 函数空间 $\Omega^X = 2^X$, 即为 $X$ 的子集的集合.

变量集合的范畴也具有这一性质, 因为它们是一般化了的 (generalized) 集合论, 即 topos. 变量集合 dynamical sets $\mathcal{S}^{\circlearrowleft}$ , graphs $\mathcal{S}^{\mathbf{\Delta}_0^{op}}$, 和 reflexive graphs $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 都是函子范畴. 它们都是 topos.

$\mathbf{C}$ 是一个范畴, 由 Yoneda 引理, $\mathbf{C}$ 可以嵌入于函子范畴 $\mathcal{S}^{\mathbf{C}^{op}}$, $C \in \mathbf{C}$, $\mathbf{C}(-,C)$ 是 $C$ 到 $\mathcal{S}$ 的一个反变函子, $\mathbf{C}(-,C) \in \mathcal{S}^{\mathbf{C}^{op}}$. $C$ 的一个 sieve $R$, 即函子 $\mathbf{C}(-,C)$ 的一个子函子, 具有性质: 对 $\mathbf{C}$ 中任一对象 $B$, $R(B) \subseteq \mathbf{C}(B,C)$; 若 $g: B \longrightarrow C, g \in R$, 对任一 $f: A \longrightarrow B$, 那么有 $g \circ f \in R(A)$. 对 $\mathbf{C}$ 中对象 $C$, 函子范畴 $\mathcal{S}^{\mathbf{C}^{op}}$ 中的真值对象 $\Omega$, $\Omega(C)$ 是 $C$ 的 sieve 的集合, 即 $\mathbf{C}(-,C)$ 子对象的集合. 若 $\alpha: B \longrightarrow C$ 为 $\mathbf{C}$ 中一个映射, 那么 $\Omega(\alpha): \Omega(C) \longrightarrow \Omega(B)$ 作用如下: $\Omega(\alpha)(R) = \alpha^{-1}(R) = \{A \xrightarrow{f} B \mid A \xrightarrow{f} B \xrightarrow{\alpha} C,\ \alpha \circ f \in R\}$. 即以下方形是 $\mathcal{S}^{\mathbf{C}^{op}}$ 中的一个 pullback 图形.

$$\begin{array}{ccc} \alpha^{-1}(R) & \hookrightarrow & B \\ \downarrow & & \downarrow \alpha \\ R & \longrightarrow & C \end{array}$$

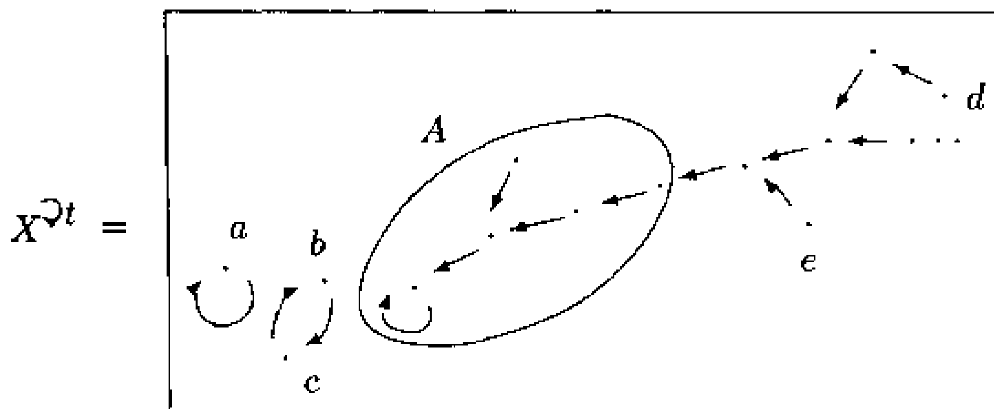
特别, 若范畴 $\mathbf{C} = M$ 是一个有单位元的半群 (monoid), 即 $M$ 是只含一个对象的范畴, $M$ 中的元素都是这个对象自到自的映射. 这样这个对象的一个 sieve 正是 $M$ 的一个右理想. $M$ 的所有右理想的集合 $\Omega$ 也是一个右 $M$- 集. 即是函子范畴 $\mathcal{S}^{M^{op}}$ 的一个对象. 若 $R$ 是 $M$ 的一个右理想, $m \in M$. $Rm = \{x \in M \mid mx \in R\}$ 也是 $M$ 的一个右理想.

例如 $M = (N,+,0)$. $N$ 的右理想 (即理想, 因为 $N$ 可换) 具有形式 $\overline{n} = \{x \in N \mid x \geqslant n\}$, 而 $\overline{n}m = \{x \in N \mid m + x \in \overline{n}\} = \begin{cases} \overline{n-m}, & m < n \\ \overline{0} = N, & m \geqslant n. \end{cases}$ 空集也是一个右理想. 我们记空集为 $\infty$. 那么在 dynamical sets 的范畴 $\mathcal{S}^{\circlearrowright} = \mathcal{S}^{N^{op}}$ 中 $\Omega$ 具有形式

$$\Omega = \{ \circlearrowleft \overline{0} \leftarrow \overline{1} \leftarrow \overline{2} \leftarrow \cdots \leftarrow \overline{n} \leftarrow \overline{n+1} \leftarrow \cdots \infty \circlearrowright \}.$$

$\Omega$ 具有两个固定点, $\overline{0}$(真) 与 $\infty$(假).

$X^{\circlearrowleft t}$ 是一个 dynamical set, $A$ 是 $X$ 的一个子系统 (sub dynamical set).




$\varphi_A:\ X \longrightarrow \Omega$, 将 $A$ 映到 $\overline{0}$, 将通过 dynamic $t$ 永远无法到达 $A$ 的部分如 $a, b, c$ 等映到 $\infty$, 而对经过 dynamic $t$ 作用 $n$ 次到达 $A$ 的点映到 $\overline{n}$, 如 $\varphi_A(d) = \overline{4}$, $\varphi_A(e) = \overline{2}$.

$\Omega = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \infty\}$ 中， $N = \overline{0}$ 代表百分之百的真， $\infty$ 代表百分之百的假，而其他真值代表在完全真与完全假之间的某种真实程度.

有单位元的半群 $\mathbf{\Delta}_1 = \{1, \partial_0, \partial_1\}$, $\partial_i\partial_j = \partial_i$, $i = 0, 1$. $\mathbf{\Delta}_1$ 的右理想有 5 个， $\Omega = \{\phi, \{\partial_0\}, \{\partial_1\}, \{\partial_0, \partial_1\}, \mathbf{\Delta}_1\}$, 其中 $\mathbf{\Delta}_1$ 与 $\phi$ 是固定点，即是退化了的箭头.

$$\{\partial_0\}\partial_0 = \{x \in \mathbf{\Delta}_1 \mid \partial_0 x = \partial_0\} = \mathbf{\Delta}_1,$$

$$\{\partial_0\}\partial_1 = \{x \in \mathbf{\Delta}_1 \mid \partial_1 x = \partial_0\} = \phi;$$

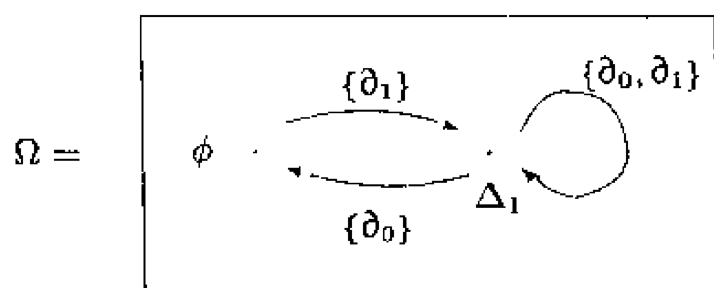
$$\{\partial_1\}\partial_0 = \{x \in \mathbf{\Delta}_1 \mid \partial_0 x = \partial_1\} = \phi,$$

$$\{\partial_1\}\partial_1 = \{x \in \mathbf{\Delta}_1 \mid \partial_1 x = \partial_1\} = \mathbf{\Delta}_1;$$

$$\{\partial_0, \partial_1\}\partial_0 = \{x \in \mathbf{\Delta}_1 \mid \partial_0 x \in \{\partial_0, \partial_1\}\} = \mathbf{\Delta}_1;$$

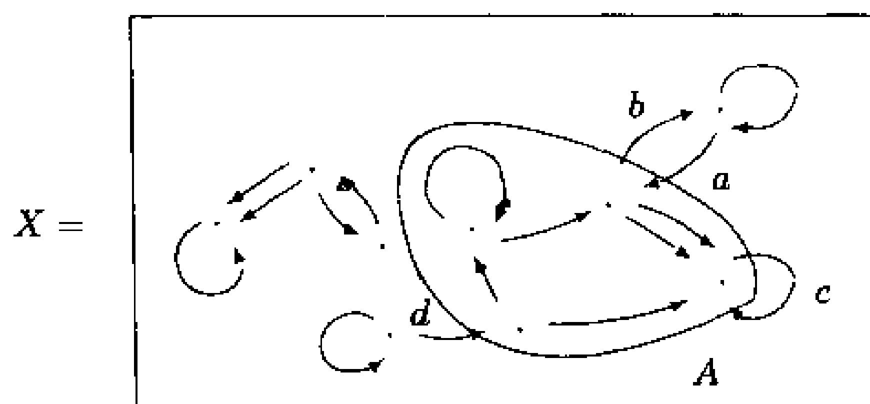
$$\{\partial_0, \partial_1\}\partial_1 = \{x \in \mathbf{\Delta}_1 \mid \partial_1 x \in \{\partial_0, \partial_1\}\} = \mathbf{\Delta}_1.$$

$\Omega =$




若 $X$ 是一个 reflexive graph, $A$ 是 $X$ 的子 graph.

$X =$




$\varphi_A : X \longrightarrow \Omega$,

$\varphi_A(A) = \mathbf{\Delta}_1$;

$\varphi_A$ 将不在 $A$ 内的点子及与 $A$ 无关的箭头映到 $\phi$;

将与 $A$ 有关的箭头 (但不在 $A$ 内),

$\varphi_A(a) = \varphi(d) = \{\partial_1\}$,

$\varphi_A(b) = \{\partial_0\}$,

$\varphi_A(c) = \{\partial_0, \partial_1\}$.

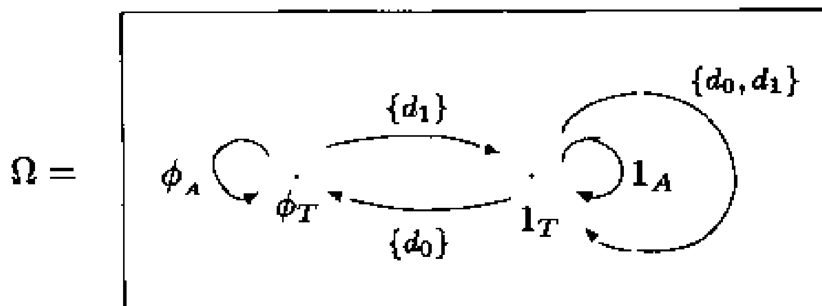
graph 范畴 $\mathcal{S}^{\mathbf{\Delta}_0^{op}}$, $\mathbf{\Delta}_0 = \left\{T \overset{d_0}{\underset{d_1}{\rightrightarrows}} A\right\}$, 范畴 $\mathbf{\Delta}_0$ 有两个对象 $T$ 与 $A$. $\Omega(T) = \{\phi, 1_T\}$, 这是 $\Omega$ 的点子. $\Omega(A) = \{\phi, \{d_0\}, \{d_1\}, \{d_0, d_1\}, 1_A\}$.

$$\Omega(A) \overset{\Omega(d_0)}{\underset{\Omega(d_1)}{\rightrightarrows}} \Omega(T).$$

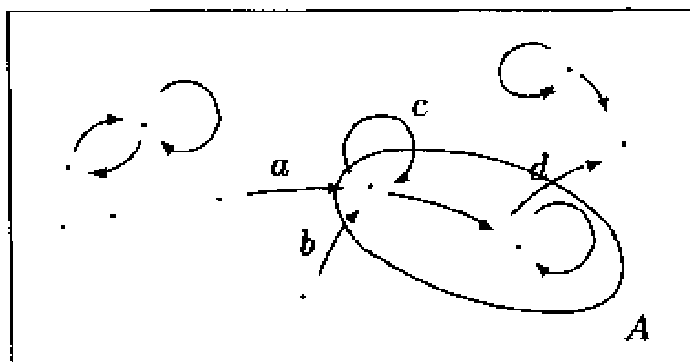
$\Omega(d_0), \Omega(d_1)$ 由以下的 pullback 图形给出. 例如对 $\{d_0\} \in \Omega(A)$,

$$
\begin{array}{ccccccc}
1_T & \longrightarrow & \{d_0\} & & \phi_T & \longrightarrow & \{d_0\} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{C}(_, T) & \xrightarrow[d_0]{} & \mathbb{C}(_, A) & & \mathbb{C}(_, T) & \xrightarrow[d_1]{} & \mathbb{C}(_, A)
\end{array}
$$

$\Omega(d_0)(\{d_0\}) = 1_T$, $\Omega(d_0)(\{d_1\}) = \phi_T$, 对 $\Omega(A)$ 中其他元素做同样的计算,




$X$ 是一个 graph, $A$ 是 $X$ 的一个子 graph.




$\varphi_A : X \longrightarrow \Omega$. $\varphi_A$ 将 $A$ 中的点子映到 $1_T$, $A$ 中的箭头映到 $1_A$; $\varphi_A$ 将 $A$ 外的点子映到 $\phi_T$, 将与 $A$ 无关的箭头映到 $\phi_A$. 而对

与 $A$ 有关又不在 $A$ 内的箭头，例如

$$\varphi_A(a)=\varphi_A(b)=\{d_1\},$$
$$\varphi_A(c)=\{d_0,d_1\},\quad \varphi_A(d)=\{d_0\}.$$

我们看到这几个变量集合的范畴 $S^{\circlearrowleft}$, $\mathcal{S}^{\Delta_0^{op}}$, 以及 $\mathcal{S}^{\Delta_1^{op}}$ 的真值对象 $\Omega$ 均不是二值的. $X$ 是一个 dynamical set, 或 graph, 或 reflexive graph, $A$ 是 $X$ 的一个子系统, $A$ 在 $X$ 中的补集, $X\setminus A$ 并不构成 $X$ 的一个子系统.

若 monoid $M$ 是一个群 $G$, 那么 $G$ 的右理想只有两个: $\phi$ 与 $G$ 本身. 这样右 $G$-set 的范畴 $\mathcal{S}^{G^{op}}$ 是布尔值的. $A$ 是 $G$-set $X$ 的子系统. 定义 $\neg A=X\setminus A=\{x\in X, x\notin A\}$. 这样 $\neg A$ 是一个 $G$-set: $x\in\neg A$, 若 $xg\in A$. 应用 $g^{-1}$: $xg\cdot g^{-1}=x(gg^{-1})=x\in A$, 这是一个矛盾. 所以 $xg\in\neg A$, $X=A\cup\neg A$.

Graph 在邮路问题与网络线路问题上有不少应用. 例如一笔画的问题等同于在一个有 $n$ 个元素的集合 $X$ 上是否存在一个到上的 dynamic $t: X\longrightarrow X$, 使得从某一点 $x_0$ 出发，若 $k,s\leqslant n$, $k\neq s$, 有 $t^k(x_0)\neq t^s(x_0)$.

Reflexive graphs $\mathcal{S}^{\Delta_1^{op}}$ 给出了很重要的一类范畴的一个简单例子, 即作为空间的范畴. 因为连通分支函子 $\pi_0: \mathcal{S}^{\Delta_1^{op}}\longrightarrow\mathcal{S}$ 保持乘积, 所以可以在 reflexive graph 上定义同伦 (homotopy).

$X,Y\in\mathcal{S}^{\Delta_1^{op}}$, 定义 $X$ 到 $Y$ 映射的同伦类为 $[X,Y]=\pi_0(Y^X)$. 这样就有了 reflexive graph 的同伦范畴: 对象是 reflexive graph, 对象 $X,Y$ 之间的映射为同伦类 $[X,Y]$. 映射之间的合成

$$\begin{aligned}[X,Y]\times[Y,Z]&=\pi_0(Y^X)\times\pi_0(Z^Y)\\&\approx\pi_0(Y^X\times Z^Y)\longrightarrow\pi_0(Z^X)=[X,Z],\end{aligned}$$

这里 $Y^X \times Z^Y \longrightarrow Z^X$ 对应于两次应用 evaluation 映射 ev,

$$\frac{Y^X \times Z^Y \longrightarrow Z^X}{X \times Y^X \times Z^Y \underset{\mathrm{ev}\times 1_{Z^Y}}{\longrightarrow} Y \times Z^Y \underset{\mathrm{ev}}{\longrightarrow} Z}.$$

这样有以下函子的可换图形

$$\begin{array}{ccc} S^{\Delta_1^{op}} & \xrightarrow{[\,,\,]} & \text{reflexive graph 的同伦范畴} \\ & {\scriptstyle \pi_0}\searrow \quad \swarrow{\scriptstyle [1,-]} & \\ & S & \end{array}$$

可以证明, $X$ 是 contractible 当且仅当对任意 $A$, $[A, X] = 1$, 当且仅当在同伦范畴内 $X \approx 1$. 因此 $X$ 是连通的, 那么 $[1, X] = 1$. 但连通的并不一定是 contractible.

将 $\pi_0(Y^X)$ 看为 discrete graph, 那么 reflexive graph 的同伦范畴是 enriched 范畴.

## 参考文献


1 Johnston P T. Topos Theory. New York: Academic Press, 1977

2 Lawvere F W, Schanuel S H. Conceptual Mathematics. Cambridge: Cambridge Univ. Press, 1997

3 Lawvere F W. Tools for the advancement of objective logic: closed categories and toposes. The Logical Foundations of Cognition (Edited by Macnamara J and Reyes G E). Oxford: Oxford Univ. Press, 1994, 43~56

# 第 13 章

# 变量集合的范畴 topos，范畴化逻辑及其应用

这一章包括以下几个小节.

1. 常量集合的范畴 $S$ 与变量集合的范畴 topos,
2. topos 与范畴化逻辑,
3. 独立性的证明,
4. 代数理论, 几何理论, 与分类 topos.

## §1 常量集合的范畴 $S$ 与变量集合的范畴 topos

常量集合的范畴 $S$ 是 ZFC 公理集合论的模型. 1964 年 Lawvere 在 "An elementary theory of the category of sets"[4] 中提出八条一阶逻辑的公理, 由这八条公理可以完全刻画常量集合范畴 $S$. 就是说, 一个范畴若满足这八条公理则等价于 (equivalent to) 集合的范畴 $S$.

以下是这八条公理.

**公理 1** 具有有限乘积 (product) 与有限和 (coproduct), 特别

有空集的乘积 terminal 对象 1, 空集的和 initial 对象 0; 任意两个映射 $A \overset{f}{\underset{g}{\rightrightarrows}} B$ 具有 equalizer 和 coequalizer.

**注 1** 公理 1 等价于有限极限与有限上极限的存在.

由于有了 terminal 对象 1, 于是可以定义一个对象的元素.

**定义 1** 对象 $A$ 的一个元素 $x$ 是由 terminal 对象 1 到 $A$ 的一个映射 $x:\ 1 \longrightarrow X$, 记为 $x \in A$.

**公理 2** 卡氏积闭合性, 即函数空间的存在. $A, B$ 是任意两个对象, 函数空间 $B^A$ 也是一个对象, 并且 $A \times X \longrightarrow B$ 一一自然对应于 $X \longrightarrow B^A$, 这里 $X$ 是任一对象, 我们用以下记号表示这一一自然对应 $\dfrac{A \times X \longrightarrow B}{X \longrightarrow B^A}$. 这就是说函子 $A \times _$ 是函子 $(\ )^A$ 的 left adjoint.

**注 2** 函数空间 $B^A$ 的元素 $1 \longrightarrow B^A$ 一一对应于 $A$ 到 $B$ 的映射 $\dfrac{1 \longrightarrow B^A}{A \longrightarrow B}$.

**公理 3** 存在自然数对象 $N$, $N$ 具有元素 $0:\ 1 \longrightarrow N$, successor 映射 $s:\ N \longrightarrow N$, 具有以下性质: 对任意对象 $X$, 以及映射 $1 \xrightarrow{x} X \xrightarrow{h} X$, 存在唯一映射 $f:\ N \longrightarrow X$, 使得 $f(0) = x$, $f \circ s = h \circ f$, 即以下图形可换

$$\begin{array}{ccccc} 1 & \xrightarrow{0} & N & \xrightarrow{s} & N \\ & \searrow^{x} & \downarrow f & & \downarrow f \\ & & X & \xrightarrow{h} & X \end{array}$$

**公理 4**(1 是 generator) $f, g:\ A \longrightarrow B$ 是两个映射. 若 $f \neq g$, 那么存在 $A$ 的元素 $x \in A$, $f(x) \neq g(x)$.

**公理 5**(选择公理) $f:\ A \longrightarrow B$ 是一映射. 若 $f$ 的定义域 $A$ 具有元素, 那么存在映射 $g:\ B \longrightarrow A$, 具有性质 $f \circ g \circ f = f$.

**公理 6** 若 $A$ 不是 initial 对象, 那么 $A$ 具有元素.

**公理 7** $A+B$ 为 $A$ 与 $B$ 的和. 若 $x\in A+B$, 那么 $x\in A$ 或 $x\in B$.

**公理 8** 存在具有多于一个元素的对象.

**注 3** 选择公理独立于其它七条公理. 让 $\mathcal{P}$ 为偏序集与保序映射的范畴. 那么 $\mathcal{P}$ 满足除公理 5 以外的七条公理. 不满足公理 5 的例: $N$ 为自然数集, 定义 $N^{\infty}=N\cup\{\infty\}, n<\infty, \forall n\in N$. $f$ 是 $N$ 到 $N^{\infty}$ 的自然嵌入, $f$ 是保序映射. 而 $N^{\infty}$ 到 $N$ 的任一保序映射 $g$ 将 $\infty$ 送到一个固定的 $n$. 这样若 $m>n$, $f(m)=m\neq f\circ g\circ f(m)$.

由于自然数对象的存在, 可以证明以下递归定理.

**定理 1**(递归定理) $A$ 是一个对象. 对于 $a: 1\longrightarrow A$, 和 $u: N\times A\longrightarrow N$, 存在唯一 $f: N\longrightarrow A$, $f(0)=a$, $f(n+1)=u(n,f(n))$.

若定义 $g: N\times A\longrightarrow N\times A$ 为 $g(n,a)=(n+1,u(n,a))$, 由 $N$ 的定义存在唯一映射 $(f_1,f): N\longrightarrow N\times A$. $f$ 正是满足定理要求的映射.

**定义 2** $A$ 是 $X$ 的一个 “子集” 当且仅当存在 $A$ 到 $X$ 的一个 monomorphism $j: A\hookrightarrow X$. $X$ 的一个元素 $x\in A$ 当且仅当存在 $\overline{x}: 1\longrightarrow A, j\circ\overline{x}=x$.

$$\begin{array}{ccc} 1 & \xrightarrow{\overline{x}} & A \\ & \searrow^{x} & \big\downarrow j \\ & & X \end{array}$$

**命题 1** 两个嵌入 $i_1: 1\longrightarrow 1+1$, $i_2: 1\longrightarrow 1+1$ 是 $1+1$ 的两个不同的元素, 并且 $1+1$ 只有这两个元素.

**定义 3** $A$ 是 $X$ 的一个子集. $A$ 的特征函数 $\varphi_A$ 是 $X$ 到 $1+1$ 的一个映射 $\varphi_A: X\longrightarrow 1+1$, 具有性质: 以下方形

$$
\begin{array}{ccc}
A & \xrightarrow{j} & X \\
\downarrow & & \downarrow \varphi_A \\
1 & \xrightarrow{i_1} & 1+1
\end{array}
$$

是一个 pullback 图形. (在 1964 年的文章中, Lawvere 的定义是 $\varphi_A$ 具有性质: 对 $X$ 的任意元素 $x$, $\varphi_A \circ x = i_1$ 当且仅当 $x \in A$. 这一要求弱于 pullback 图形的要求. 但是当我们定义了广义元素之后 (第二节), 这两个定义是等价的.)

**注 4** 由于 equalizer 的存在, $X$ 到 $1+1$ 的任一映射 $\varphi : X \longrightarrow 1+1$ 对应于 $X$ 的一个子集. 因而 $\varphi$ 是一个特征函数.

**命题 2** $X$ 的任一子集具有特征函数.

证明见 [4].

于是可以称 $1+1$ 为子集的 classifier.

公理 1, 公理 2 以及任一对象 $X$ 的子集一一对应于 $X$ 到 $1+1$ 的映射. 这正是 topos 的三条定义. 而 $1+1$ 为子集 classifier 等价于这一 topos 是布尔的.

Lawvere 研究常量集合的范畴 $S$ 的公理化是为了了解变量集合与常量集合的共同性与特殊性, 进而公理化变量集合的范畴. 几何中的各种结构如代数簇, 复盖空间, 层 (sheaf), 纤维丛等都是变量的集合.

通常研究变化运动的事物, 我们总是先将其孤立静止到常量的集合, 再加上某种结构, 使之连贯运动起来. 就像电影胶带, 本身是一格一格静止的照片, 快速放映起来就成了运动的电影. Lawvere 的思想是, 世界本身是变化的相互联系的. 我们应该能够把变化着的联系着的事物直接作为学习研究的对象, 而不必总是回到静止和孤立的常量集合中去. 变量集合的范畴本身就是一个 universe, 我们可以在其内直接做逻辑、推理、以及各种数学构造.

Grothendieck 注意到一个拓扑空间的开复盖族的性质，提出了一个小范畴 C 上的拓扑的概念. C 是一个小范畴, $J$ 是 C 中对象的一个"开"复盖族称为 C 一个 Grothendieck 拓扑. 若 C 是一个拓扑空间的开集构成的 poset, 那原空间的开复盖族构成一个 Grothendieck 拓扑. 我们可以构造 $(\mathbf{C}, J)$ 上 sheaf 的范畴 $\mathrm{sh}(\mathbf{C}, J)$. 任一范畴等价于 $\mathrm{sh}(\mathbf{C}, J)$, 称为 Grothendieck topos.

Giraud 公理化了 Grothendieck topos, 给出以下的等价定理.

**定理 2**(Giraud) $\mathcal{E}$ 是一个范畴. 以下两条等价.

1. $\mathcal{E}$ 是一个 Grothendieck topos.

2. $\mathcal{E}$ 满足以下条件.

(1) $\mathcal{E}$ has finite limits.

(2) $\mathcal{E}$ has all set-indexed coproducts, and they are disjoint and universal.

(3) Equivalence relations in $\mathcal{E}$ have universal coequalizer.

(4) Every equivalence relation in $\mathcal{E}$ is effective, and every epimorphism is a coequalizer.

(5) $\mathcal{E}$ has small hom-sets.

(6) $\mathcal{E}$ has a set of generators.

常量集合的范畴 $S$ 可以看为是一个元素的拓扑空间上的 sheaf 的范畴.

1971 年 Lawvere 和 Tierney 在研究了 Grothendieck topos 之后提出 elementary topos 的概念.

**定义 4** $\mathcal{E}$ 是一个范畴. 若 $\mathcal{E}$ 满足以下条件, 那么 $\mathcal{E}$ 是一个 topos.

1. $\mathcal{E}$ 具有有限极限.

2. $\mathcal{E}$ 是卡氏积闭合的. 这是说, 对 $\mathcal{E}$ 的任一对象 $X$, 函数空间函子 $(\ )^X : \mathcal{E} \longrightarrow \mathcal{E}$ 是函子 $(\ ) \times X : \mathcal{E} \longrightarrow \mathcal{E}$ 的 right adjoint.

3. $\mathcal{E}$ 具有子对象 classifier $\Omega$, 即对 $\mathcal{E}$ 中任一 monomorphism

$a: A \hookrightarrow X$, $a$ 有特征函数 $\varphi_a: X \longrightarrow \Omega$, 使得以下图形为一个 pullback

$$\begin{array}{ccc} A & \overset{a}{\hookrightarrow} & X \\ \downarrow & & \downarrow \varphi_a \\ 1 & \overset{t}{\longrightarrow} & \Omega \end{array}$$

这里 $t: 1 \longrightarrow \Omega$ 代表真.

Topos 即是公理化的变量集合的范畴. Topos 包括 Grothendieck topos, 特别常量集合的范畴 $S$ 是一个 topos.

## §2 Topos 和范畴化逻辑 (categorical logic)

经典逻辑或二值逻辑是建立在常量集合的范畴 $S$ 上的. 一般 topos 是变量集合的范畴, 变量集合的逻辑是多值逻辑. 称为 intuitionistic logic. 这里借用 intuitionistic 的名字, 变量集合的逻辑即 topos 的逻辑与 Brouwer 为代表的唯心的 intuitionists 的逻辑在某些方面的一致只是一个偶然的重合.

$X$ 是一个常量集合, $X$ 的一个元素 $x \in X$ 是从一个元素的集合 1 到 $X$ 的一个映射, $x: 1 \longrightarrow X$. 一个常量的集合可以完全由它的元素来刻画, 但对变量的集合 (或非常量的集合), 这却是不够的. 例如 $X$ 是一个几何空间. 要了解 $X$ 我们需要知道 $X$ 中的各维图形, 而不只是 0- 维图形 (点)$1 \longrightarrow X$; 我们需要了解一维图形 (线段) $I_1 \longrightarrow X$, 这里 $I_1$ 是单位区间或任意有限闭区间; 二维图形 $I_2 \longrightarrow X$, $I_2$ 是任意简单有限闭二维图形; $\cdots$; $n$ 维图形 $I_n \longrightarrow X$, $I_n$ 是任意简单有限闭 $n$ 维图形.

这样需要将常量集合的元素概念推广. $X$ 的一个元素 (广义元素, generalized element) 是一个以 $X$ 为 codomain 的映射

$x: T \longrightarrow X$, 记为 $x \in X$. 若 domain 为 terminal 对象 $x: 1 \longrightarrow X$, 称这样的元素为 global element. $A$ 是 $X$ 的一个子对象 (子集) 即存在 $A$ 到 $X$ 的一个 monomorphism $j_A: A \longrightarrow X$. $X$ 的一个元素 $x \in X$, $x \in A$ 当且仅当存在 $a: T \longrightarrow A$, 并且 $j_A \circ a = x$

$$\begin{array}{ccc} T & \xrightarrow{a} & A \\ & \underset{x}{\searrow} & \downarrow j_A \\ & & X \end{array}$$

若 $j_B: B \longrightarrow X$ 是 $X$ 的另一子对象. 那么 $A \subseteq B$ 当且仅当存在 $g: A \longrightarrow B$, 并且 $j_A = j_B \circ g$

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle j_A}\searrow & & \swarrow{\scriptstyle j_B} \\ & X & \end{array}$$

这样我们有了所熟悉的 $\in, \subseteq$ 语言.

记 $X$ 的子对象的集合为 $\mathrm{sub}(X)$. $\mathrm{sub}(X)$ 是一个 poset. 由 $\Omega$ 的定义, $\mathrm{sub}(X) \approx \mathcal{E}(X, \Omega)$, 这就是说 $X$ 的子对象可以由 $\Omega$ 来代表. 为了研究 $\mathrm{sub}(X)$ 以及 $\Omega$ 的性质与结构, 我们需要以下两个有关 topos 的基本定理.

**定理 3** Topos $\mathcal{E}$ 中的任一映射 $f: X \longrightarrow Y$ 可以分解为一个 epimorphism 与一个 monomorphism 的复合

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \searrow & & \nearrow \\ & \mathrm{Im}\, f & \end{array}$$

这一分解在同构意义下唯一的. 这一分解称为象分解 (image factorization).

**定理 4** $\mathcal{E}$ 是一个 topos. $f:\ X \longrightarrow Y$ 是 $\mathcal{E}$ 中一个映射. $f$ 诱导的 pullback 函子 $f^*:\ \mathcal{E}/Y \longrightarrow \mathcal{E}/X$ 具有两个 adjoint, $\Sigma_f:\ \mathcal{E}/X \longrightarrow \mathcal{E}/Y$ 是 $f^*$ 的 left adjoint, $\Pi_f:\ \mathcal{E}/X \longrightarrow \mathcal{E}/Y$ 是 $f^*$ 的 right adjoint, 并且 $f^*$ 是 logical(保持有限极限, 函数空间, 以及子对象 classifier)

例如, 若 $\mathcal{E} = S$ 为常量集合的范畴, comma 范畴或 slice 范畴 $S/X$ 中的任一对象: $h:\ A \longrightarrow X$, 可以看为是以 $X$ 的元素为指数 (index) 的子集族

$$h = \{h_x \mid x \in X\}, \quad h_x = h^{-1}(x) = \{a \in A \mid h(a) = x\}.$$

若 $g:\ B \longrightarrow Y$ 是 $\mathcal{E}/Y$ 中的一个对象, $g = \{g_y \mid y \in Y\}$, 那么

$$\begin{aligned} &f^*(g)_x = g_{f(x)}, \\ &\Sigma_f(h)_y = \coprod_{f(x)=y} g_x \qquad \text{“}\exists x\ f(x) = y\text{''} \\ &\Pi_f(h)_y = \prod_{f(x)=y} g_x \qquad \text{“}\forall x\ f(x) = y\text{''}. \end{aligned}$$

因为 $\Pi_f$ 具有 left adjoint $f^*$, 所以 $\Pi_f$ 保持 monomorphism, 限制 $\Pi_f$ 于 $\mathrm{sub}(X)$, 我们得到 $\forall_f$: $\mathrm{sub}(X) \longrightarrow \mathrm{sub}(Y)$.

$\Sigma_f(h) = f \circ h:\ A \longrightarrow X \longrightarrow Y$, 取 $f \circ h$ 的象分解, 记 $\mathrm{Im}\, f \circ h = \exists_f(h)$.

于是有

$$\mathrm{sub}(X) \underset{\Pi_f}{\overset{\exists_f}{\underset{\longleftarrow\, f^* \,}{\longrightarrow}}} \mathrm{sub}(Y)$$

$\exists_f$ 是 $f^*$ 的 left adjoint, $f^*$ 是 $\Pi_f$ 的 left adjoint. 特别对投影 $f = \Pi_Y: X \times Y \longrightarrow Y$, 有

$$\mathrm{sub}(X \times Y) \underset{\forall_{\Pi_Y} = \forall_X}{\overset{\exists_{\Pi_Y} = \exists_x}{\underset{\longleftarrow\, \Pi_Y^* \,}{\longrightarrow}}} \mathrm{sub}(Y)$$

**定理 5** sub($X$) 是一个格.

**证明** 恒等映射 $1_X: X \longrightarrow X$ 是最大元, $0: 0 \longrightarrow X$ 是最小元.

$j_A: A \longrightarrow X, j_B: B \longrightarrow X$ 是 $X$ 的两个子对象. 它们的 pullback 即是它们的交. 为构造它们的并, 先构造和 $A+B$. 由和的 universal 性质, 存在 $A+B$ 到 $X$ 的映射 $\tau: A+B \longrightarrow X$

$$\begin{array}{ccc} A+B & \longleftarrow & B \\ \uparrow & \searrow^{\tau} & \downarrow j_B \\ A & \xrightarrow[j_A]{} & X \end{array}$$

使得两个三角形均可换. 做 $\tau: A+B \longrightarrow X$ 的象分解, 即为 $j_A, j_B$ 的并.

$$\begin{array}{ccc} A+B & \xrightarrow{\tau} & X \\ & \searrow \quad \nearrow & \\ & \mathrm{Im}\,\tau = A \cup B & \end{array}$$

通过直接计算可知，如上定义的运算确定构成一个格.

我们知道 $\Omega$ 是 topos $\mathcal{E}$ 的真值对象. 常量集合的 topos $S$ 的真值对象 $\Omega = 2 = 1 + 1$, 而对一个一般 topos 的 $\Omega$ 有以下定理

**定理 6** $\Omega$ 是一个 internal Heyting algebra.

**证明** $t: 1 \longrightarrow \Omega$ 是最大元， $f: 1 \longrightarrow \Omega$ 是最小元，这里 $f$ 是 $0 \longrightarrow 1$ 的特征函数；而 $f$ 的特征函数 $\neg: \Omega \longrightarrow \Omega$ 是 negation; $(t,t): 1 \longrightarrow \Omega\times\Omega$ 的特征函数是和取 $\wedge: \Omega\times\Omega \longrightarrow \Omega$; 做 $1\times t: \Omega\times 1 \longrightarrow \Omega\times\Omega$ 与 $t\times 1: 1\times\Omega \longrightarrow \Omega\times\Omega$ 的并，它的特征函数即是 $\Omega$ 的析取 $\vee: \Omega\times\Omega \longrightarrow \Omega$; 蕴涵 $\Longrightarrow$ 是 $\Omega$ 的序关系 $\Omega_1$ 的特征函数. 这里序关系 $\Omega_1$ 是 equalizer $\Omega_1 \longrightarrow \Omega\times\Omega \overset{\wedge}{\underset{\pi_1}{\rightrightarrows}} \Omega$.

通过直接计算可以验证以上定义的 $t, f, \neg, \wedge, \vee, \Longrightarrow$ 满足 Heyting 代数的要求.

**推论** 由于 $\mathrm{sub}(X) \approx \mathcal{E}(X,\Omega)$, 所以 $\mathrm{sub}(X)$ 是一个 Heyting 代数 (external), 而 $\Omega^X$ 是一个 internal Heyting 代数.

Topos 中的逻辑是所谓的 intuitionistic type theory. Topos $\mathcal{E}$ 中的每一个对象 $X$ 是一个类型，类型 $X$ 具有可数多个变量 $x$, 记为 $x: X$, 或 $x \in X$, 表示 $x$ 是以 $X$ 为类型的变量. $x$ 的解释是 $X$ 到 $X$ 的恒等映射 $1_X: X \longrightarrow X$. 每一个变量是一个项 (term). 一个一般项含有自由变量以及具有类型 (type). 例如项 $s$ 具有自由变量 $y, z, w$, 以及类型 $X$, 通常记为 $s(y,z,w) \in X$, 而 $s$ 的解释是映射 $s: Y\times Z\times W \longrightarrow X$. 特别以 $\Omega$ 为类型的项称为公式 (formula).

项有如下构造法.

1. 若 $s, t$ 分别是以 $X, Y$ 为类型的项， $s: U \longrightarrow X$, $t: V \longrightarrow Y$, 那么 $(s,t): U\times V \longrightarrow X\times Y$, $(s,t)$ 是以 $X\times Y$ 为类型的项.

2. 若 $s, t$ 都是以 $X$ 为类型的项，那么 $s = t$ 是以 $\Omega$ 为类型的项，即是一个公式. $s = t$ 的解释为 $U\times V \xrightarrow{(s,t)} X\times X \xrightarrow{\delta_X} \Omega$, 这里 $\delta_X$ 是对角线映射 $\Delta: X \longrightarrow X\times X$ 的特征函数.

3. $s$ 是一个以 $X$ 为类型的项，$f: X \longrightarrow Y$ 是 $\mathcal{E}$ 中的映射，那么 $f \circ s: U \xrightarrow{s} X \xrightarrow{f} Y$ 是以 $Y$ 为类型的项.

4. $s: U \longrightarrow X, t: V \longrightarrow Y^X$ 是项，那么 $t(s)$ 是以 $Y$ 为类型的项，$t(s): U \times V \xrightarrow{(s,t)} X \times Y^X \xrightarrow{\mathrm{ev}} Y$, 这里 ev: $X \times Y^X \longrightarrow Y$ 称为 evaluation 是 $1_{Y^X}: Y^X \longrightarrow Y^X$ 的 transpose.

5. $x$ 是以 $X$ 为类型的变量，$s: X \times U \longrightarrow Y$ 是一个项，那么 $\lambda_x.s$ 是一个以 $Y^X$ 为类型的项. $\lambda_x.s: U \longrightarrow Y^X$ 是 $X \times U \longrightarrow Y$ 的 transpose.

对公式定义有二元运算 $\wedge, \vee, \Longrightarrow$, 和一元运算 $\neg$. 让 $\varphi, \psi$ 为公式，$\varphi: X \longrightarrow \Omega, \psi: Y \longrightarrow \Omega$, 那么

$$\varphi \wedge \psi: X \times Y \xrightarrow{(\varphi,\psi)} \Omega \times \Omega \xrightarrow{\wedge} \Omega$$

$$\varphi \vee \psi: X \times Y \xrightarrow{(\varphi,\psi)} \Omega \times \Omega \xrightarrow{\vee} \Omega$$

$$\varphi \Longrightarrow \psi: X \times Y \xrightarrow{(\varphi,\psi)} \Omega \times \Omega \xrightarrow{\Rightarrow} \Omega$$

$$\neg\varphi: X \xrightarrow{\varphi} \Omega \xrightarrow{\neg} \Omega$$

$\varphi(x,y): X \times Y \longrightarrow \Omega, \forall_{x \in X}\varphi(x,y)$ 的解释是

$$Y \xrightarrow{\overline{\varphi}} \Omega^X \xrightarrow{\forall_x} \Omega.$$

而 $\exists_{x \in X}\varphi(x,y)$ 的解释是 $Y \xrightarrow{\overline{\varphi}} \Omega^X \xrightarrow{\exists_x} \Omega$, 这里 $\forall_x, \exists_x$ 分别是 $X \longrightarrow 1$ 诱导的 $\Omega \longrightarrow \Omega^X$ 的 internal right adjoint 和 left adjoint.

一个公式 $\varphi: X \longrightarrow \Omega$ 对应于 $X$ 的一个子对象 $\{x \mid \varphi(x)\}$. $\varphi$ 为真，当且仅当 $\varphi$ 对应于 $X$ 的最大子对象 $1_X$. $\varphi$ 为真记为 $\mathcal{E} \vDash \varphi$, 或 $\vDash \varphi$. 特别对于闭公式 $\varphi$, $\varphi$ 为真当且仅当 $\varphi = t: 1 \longrightarrow \Omega$.

这样对公式 $\forall_{x \in X}\varphi(x,y)$ 与 $\exists_{x \in X}\varphi(x,y)$ 又有如下解释. $\{(x,y) \mid \varphi(x,y)\}$ 是 $X \times Y$ 的子对象. 应用 adjoints $\forall_{\Pi_Y} = \forall_x$, $\exists_{\Pi_Y} = \exists_x$ : $\mathrm{sub}(X \times Y) \longrightarrow \mathrm{sub}(Y)$, 我们得到与 $\forall_{x \in X}\varphi(x,y)$, $\exists_{x \in X}\varphi(x,y)$ 相对应的 $Y$ 的子对象 $\forall_x\{(x,y) \mid \varphi(x,y)\}$, $\exists_x\{(x,y) \mid \varphi(x,y)\}$, 即以下两个方形均为 pullback 图形.

$$\begin{array}{ccc}\forall_x\{(x,y)|\varphi(x,y)\} & \longrightarrow & Y \\ \downarrow & & \downarrow \forall_{x\in X}\varphi(x,y) \\ 1 & \xrightarrow{t} & \Omega\end{array}$$

$$\begin{array}{ccc}\exists_x\{(x,y)|\varphi(x,y)\} & \longrightarrow & Y \\ \downarrow & & \downarrow \exists_{x\in X}\varphi(x,y) \\ 1 & \xrightarrow{t} & \Omega\end{array}$$

由于 $\Omega$ 的存在，$\in, \subseteq$ 的相应定义，在 topos 中，我们可以像在集合的范畴 $S$ 中那样做通常的推理证明，只是需要注意不要用到反证法，这是因为排中律在 topos 中一般不成立．而且不要用到选择公理．下而是几个应用范畴化逻辑的例子．

$\mathcal{E}$ 是一个 topos．$f: X \longrightarrow Y$ 是 $\mathcal{E}$ 中的一个映射．以下这几个命题都是对的．

**命题 3** $f$ 是一个 monomorphism, 当且仅当

$$\vDash \forall_{x_1\in X}\ \forall_{x_2\in X}(f(x_1) = f(x_2) \Longrightarrow x_1 = x_2).$$

**命题 4** $f$ 是一个 epimorphism, 当且仅当

$$\vDash \forall_{y\in Y}\ \exists_{x\in X}(f(x) = y).$$

**命题 5** 若 $\vDash \forall_{x\in X}\exists!_{y\in Y}\varphi(x,y)$, 那么存在映射 $f: X \longrightarrow Y$, 使得 $\vDash \forall_{x\in X}\varphi(x, f(x))$.

Topos 的逻辑语言在 sheaf 构成的 topos 中有自然的类似于在集合的 topos $S$ 中的语义解释．例如 $\mathcal{E} = S^{\mathbf{U}^{op}}$, 这里 $\mathbf{U}$ 是一个拓扑空间的开集构成的偏序集．$\varphi(x)$ 是一个公式，含有自由变量 $x \in X$, 那么 $\{x \mid \varphi(x)\}$ 是 $X$ 的一个子对象，即 $X$ 的子 sheaf. $a: U \longrightarrow X$, 即 $a \in X$. 由 Yoneda 引理, 作为集合 $X(U) = \mathcal{E}(U, X)$,

$a \in X(U)$. 这样， $a \in \{x \mid \varphi(x)\}$ 当且仅当 $a \in \{x \mid \varphi(x)\}(U)$. 我们记 $a \in \{x \mid \varphi(x)\}(U)$ 为 $U \Vdash \varphi(a)$ 或 $\Vdash \varphi(a)$.

对于复合的公式有以下自然的解释.

1. $\Vdash \varphi(a) \wedge \psi(a)$ 当且仅当 $\Vdash \varphi(a)$ 并且 $\Vdash \psi(a)$.

2. $\Vdash \varphi(a) \vee \psi(a)$ 当且仅当存在 $U$ 的一个开复盖 $\{U_i \xrightarrow{a_i} U\}$, 对任意 $i, \Vdash \varphi(aa_i)$ 或 $\Vdash \psi(aa_i)$.

3. $\Vdash (\varphi(a) \Longrightarrow \psi(a))$ 当且仅当对于任意 $g: V \longrightarrow U$, 若 $\Vdash \varphi(ag)$, 那么 $\Vdash \psi(ag)$.

4. $\Vdash \neg\varphi(a)$ 当且仅当若 $g: V \longrightarrow U, \Vdash \varphi(ag)$, 那么 $V = \phi$.

5. $\varphi(x, y)$ 有两个自由变量, 对于 $a \in X(U), \Vdash \exists_y \varphi(a, y)$ 当且仅当存在 $U$ 的一个开复盖 $\{U_i \xrightarrow{a_i} U\}$, $b_i \in Y(U_i)$, 使得 $\Vdash \varphi(aa_i, b_i)$.

6. $\Vdash \forall_y \varphi(a, y)$ 当且仅当对任意 $g: V \longrightarrow U$ 以及任意 $b \in Y(V), \Vdash \varphi(ag, b)$.

这个语义解释对任一 Grothendieck topos $\mathrm{sh}(\mathbb{C}, J)$ 都是对的.

## §3 独立性的证明

利用 topos, 可以证明选择公理独立于连续统假设，选择公理独立于 ZF 公理系统. 这两个独立性的证明都依赖于 topos 内的拓扑结构. 这里我们首先介绍一个 topos $\mathcal{E}$ 中的拓扑的概念以及相应于这一拓扑的 sheaf 的 topos.

$X$ 是一个拓扑空间， $\mathbf{U}$ 是 $X$ 的开集构成的 poset, 因而是一个范畴. $X$ 上的 sheaf 的范畴 $\mathrm{sh}(X)$ 是函子范畴 $S^{\mathbf{U}^{op}}$ 的一个子范畴， $\mathrm{sh}(X)$ 和 $S^{\mathbf{U}^{op}}$ 均为 topos.

拓扑空间 $X$ 上的 sheaf 是建立在开复盖的概念之上的. $U$ 是 $X$ 的一个开集， $\{1_U: U \longrightarrow U\}$ 是 $U$ 的最大开复盖; 若 $\{U_i \longrightarrow U\}_i$ 是 $U$ 的一个开复盖， $V \subseteq U$, 那么 $\{U_i \cap V \longrightarrow V\}_i$ 是 $V$ 的一个开复盖; $\{U_i \longrightarrow U\}_i$ 是 $U$ 的一个开复盖， $\{U_\alpha \longrightarrow U\}_\alpha$

是 $U$ 的一个开子集族. 若对任意 $U_i \longrightarrow U$, $\{U_i \cap U_\alpha \longrightarrow U\}_\alpha$ 是 $U_i$ 的一个开复盖, 那么 $\{U_\alpha \longrightarrow U\}_\alpha$ 是 $U$ 的一个开复盖.

推广了开复盖的这些性质, Grothendieck 提出了一个小范畴 $\mathbb{C}$ 上的拓扑的概念.

由 Yoneda 引理, $\mathbb{C}$ 中任一对象 $C$ 是函子范畴 $S^{\mathbb{C}^{op}}$ 的一个对象, $C$ 在 $S^{\mathbb{C}^{op}}$ 中的子对象称为 $C$ 的 sieve. 若 $\mathbb{C} = \mathbf{U}$, 那么 $U$ 的一个开复盖是 $U$ 的一个 sieve.

范畴 $\mathbb{C}$ 上的一个 Grothendieck 拓扑是一个 $\mathbb{C}$ 中对象的 sieve 族 $J$. 对 $\mathbb{C}$ 中任一对象 $C$, $J(C)$ 是 $C$ 的 sieve 的一个集合, $J(C)$ 中的 sieve 称为 $C$ 的一个复盖. 这样 $J(C)$ 是 $\Omega(C)$ 的子集 ($\Omega(C)$ 是 $C$ 的所有 sieve 的集合). $J$ 满足以下条件

1) $\{1_C\} \in J(C)$.

2) $R \in J(C)$, 对任意 $f: B \longrightarrow C$, $f^*(R) \in J(B)$. 这里 $f^*(R)$ 是 pullback

$$\begin{array}{ccc} f^*(R) & \hookrightarrow & B \\ \downarrow & & \downarrow f \\ R & \hookrightarrow & C \end{array}$$

3) $R \in J(C)$, $S$ 是 $C$ 的一个 sieve, 若对任意 $g \in R$, $g: B \longrightarrow C$, $g^*(S) \in J(B)$, 那么 $S \in J(C)$.

$F \in S^{\mathbf{U}^{op}}$, $U \in \mathbf{U}$, $\{U_i\}$ 是 $U$ 的一个开复盖, $F$ 的一个 compatible family 是一族元素 $s_i \in F(U_i)$, 并且 $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$. 进而, $F$ 是一个 sheaf, 若对任一这样的 compatible family 存在 $s \in F(U)$, 并且 $s|_{U_i} = s_i$.

函子范畴 $S^{\mathbb{C}^{op}}$ 中的对象称为 presheaf. Presheaf $F$ 的一个 compatible family 定义如下: $C$ 是 $\mathbb{C}$ 的一个对象, $R \in J(C)$ 是 $C$ 的一个复盖, 对 $g \in R(A)$, 即 $g: A \longrightarrow C$, 存在 $F(A)$ 中的元素

$\tau(g)$, 满足性质：若 $f:\ B \longrightarrow A$, 那么 $\tau(g\circ f)=F(f)(\tau(g))$, 就是说以下方形可换

$$\begin{array}{ccc} R(A) & \xrightarrow{\tau} & F(A) \\ \downarrow {\scriptstyle -\circ f} & & \downarrow {\scriptstyle F(f)} \\ R(B) & \xrightarrow{\tau} & F(B) \end{array}$$

这正是说 $\tau$ 是 $R$ 到 $F$ 的一个自然变换.

这样， $F$ 是 $(\mathbb{C},J)$ 上的一个 sheaf, 若对任一 $R\in J(C)$, $R$ 到 $F$ 的一个自然变换 $R\longrightarrow F$ 具有唯一扩张 $C\longrightarrow F$,

$$\begin{array}{ccc} R & \longrightarrow & F \\ \downarrow & \nearrow_{\exists !} & \\ C & & \end{array}$$

$(\mathbb{C},J)$ 上的 sheaf 以及它们之间的自然变换构成 $S^{\mathbb{C}^{op}}$ 的一个子范畴 $\mathrm{sh}(\mathbb{C},J)$, $\mathrm{sh}(\mathbb{C},J)$ 也是一个 topos.

$\mathcal{E}=\mathrm{sh}(\mathbb{C},J)$, 由 Grothendieck 拓扑定义中的第二条， $J$ 是 $\Omega$ 的一个子对象，即 $J$ 有特征函数 $j:\ \Omega\longrightarrow\Omega$. 对于 $S\in\Omega(C)$, $j_C(S)=\{g:\ D\longrightarrow C \mid g^*(S)\in J(D)\}$. 显然 $j_C(1_C)=1_C$; 不难直接证明 $j_C\circ j_C(S)=j_C(S)$, 并且 $j_C(R\cap S)=j_C(R)\cap j_C(S)$. 这样 Lawvere–Tierney 提出了一个 topos $\mathcal{E}$ 内的拓扑的概念.

**定义 5** $\mathcal{E}$ 是一个 topos. $\mathcal{E}$ 的一个拓扑是 $\Omega$ 的一个子对象 $J$, $J$ 的特征函数 $j:\ \Omega\longrightarrow\Omega$ 满足

1) $j\circ t=t$

$$\begin{array}{ccc} 1 & \xrightarrow{t} & \Omega \\ & {\scriptstyle t}\searrow & \downarrow {\scriptstyle j} \\ & & \Omega \end{array}$$

2) $j \circ j = j$

$$\begin{array}{ccc} \Omega & \xrightarrow{j} & \Omega \\ & \searrow_{j} & \downarrow j \\ & & \Omega \end{array}$$

3) $j \circ \wedge = \wedge \circ j \times j$

$$\begin{array}{ccc} \Omega \times \Omega & \xrightarrow{\wedge} & \Omega \\ \downarrow j \times j & & \downarrow j \\ \Omega \times \Omega & \xrightarrow{\wedge} & \Omega \end{array}$$

$j:\ \Omega \longrightarrow \Omega$ 给出一个闭包运算： $A \in \mathrm{sub}(E)$, $A$ 的 $j$- 闭包 $\overline{A}$ 的特征函数 $\mathrm{char}\, \overline{A} = j \circ \mathrm{char}\,(A)$. 若 $\overline{A} = E$, 则称 $A$ 为 dense(或 $j$-dense). 例如 $\mathcal{E} = \mathrm{sh}\,(\mathbb{C}, J)$, $R \in J(C)$, $R \hookrightarrow C$ 为 dense. $\mathcal{E}$ 中对象 $F$ 是一个 $j$-sheaf, 若对任意 $j$-dense $A \hookrightarrow E$, 以及 $\tau:\ A \longrightarrow F$, 存在唯一扩张 $\overline{\tau}:\ E \longrightarrow F$,

$$\begin{array}{ccc} A & \xrightarrow{\tau} & F \\ \downarrow & \nearrow_{\overline{\tau}} & \\ E & & \end{array}$$

$\mathcal{E}$ 中的 $j$-sheaf 以及它们之间的映射构成 $\mathcal{E}$ 的一个子范畴 $\mathcal{E}_j$, $\mathcal{E}_j$ 也是一个 topos.

**定理 7** $\mathbb{C}$ 是一个小范畴. $\mathbb{C}$ 上的 Grothendieck 拓扑一一对应于 $S^{\mathbb{C}^{op}}$ 中的 Lawvere–Tierney 拓扑. 并且 $\mathrm{sh}(\mathbb{C}, J) \approx \mathcal{E}_j$.

**定理 8** Inclusion 函子 $\mathcal{E}_j \longrightarrow \mathcal{E}$ 有一个 left adjoint $L:\ \mathcal{E} \longrightarrow \mathcal{E}_j$, $L$ 称为 sheafification 函子. $L$ 是 left exact (保持有限极限).

Negation $\neg:\ \Omega \longrightarrow \Omega$, 不难检验 $\neg\neg = \neg \circ \neg:\ \Omega \longrightarrow \Omega$ 是 $\mathcal{E}$ 的一个拓扑. 这样我们可以构造 $\neg\neg$-sheaf 的 topos $\mathcal{E}_{\neg\neg}$. 两个独立性的证明都依赖于这种 double negation sheaf 的 topos $\mathcal{E}_{\neg\neg}$.

**定理 9** Topos $\mathcal{E}_{\neg\neg}$ 是布尔的, 并且 $\mathcal{E}_{\neg\neg}$ 是 $\mathcal{E}$ 中最好的布尔逼迁.

Lawvere 与 Tierney 用 $\neg\neg$-sheaf topos, 与 Cohen 类似的力迫 (forcing) 方法证明了连续统假设与选择公理的独立性. P. Freyd 用另一种 $\neg\neg$-sheaf topos 证明了选择公理与集合论一般公理的独立性.

$\mathbf{N}$ 是自然数集, $2^{\mathbf{N}}$ 是 $\mathbf{N}$ 的子集的集合, $2^{\mathbf{N}}$ 具有与实数集 $\mathbf{R}$ 相同的基数.

取 $B$ 为一个集合. 其基数大于 $2^{\mathbf{N}}$ 的基数. 例如 $B$ 可以是 $2^{2^{\mathbf{N}}}$. 构造集合论的另一模型, 在这一模型中, 若我们能找到 $B$ 到 $2^{\mathbf{N}}$ 的一个单射 $g: B \longrightarrow 2^{\mathbf{N}}$, 并且证明不存在 $\mathbf{N}$ 到 $B$, 以及 $B$ 到 $2^{\mathbf{N}}$ 的满射, $\mathbf{N} < B < 2^{\mathbf{N}}$, 这样就给出连续统假设的一个反例. 映射 $g$ 相当于 $f: B \times \mathbf{N} \longrightarrow 2$. 当然这样的单射 $g$ 或 $f$ 是不存在的 (Cantor's diagonal argument). 但是我们可以取 $f$ 的有限逼近. $g$ 为单射, 即若 $b_1 \neq b_2$, 那么存在 $n$ 使得 $f(b_1, n) \neq f(b_2, n)$. $f$ 的一个有限逼近是 $B \times \mathbf{N}$ 的一个有限子集 $F_p$, 以及 $F_p$ 到 2 的一个映射 $p: F_p \longrightarrow 2$. 定义 $q \leqslant p$ 当且仅当 $F_p \subseteq F_q$, 并且 $q|_{F_p} = p$. 这样 $f$ 的有限逼近构成一个偏序集 $\mathbf{P}$. 构造 sheaf 范畴 $\mathrm{sh}(\mathbf{P}, \neg\neg)$. Topos $\mathrm{sh}(\mathbf{P}, \neg\neg)$ 称为 Cohen topos.

**命题 6** Cohen topos $\mathrm{sh}(\mathbf{P}, \neg\neg)$ 是布尔的, 并且选择公理成立.

我们知道任一布尔的 Grothendieck topos 是 Zermelo–Frankel 集合论的一个模型. Cohen topos $\mathrm{sh}(\mathbf{P}, \neg\neg)$ 正是我们的集合论的新模型. $\mathrm{sh}(\mathbf{P}, \neg\neg)$ 具有自然数对象 $\mathbf{N}$. 我们要构造一个 $\neg\neg$-sheaf $K$ 以及两个映射 $\mathbf{N} \longrightarrow K$, $K \longrightarrow \Omega^{\mathbf{N}}$, 这两个映射均为 monomorphism, 并且我们证明不存在 epimorphism $\mathbf{N} \longrightarrow K$, 以及 $K \longrightarrow \Omega^{\mathbf{N}}$. 这样, $K$ 的存在使连续统假设不成立.

$\Delta: S \longrightarrow S^{\mathbf{P}^{op}}$ 是常量函子. 将任一集合 $s$ 送到相应的常量函子 $\Delta s$, $\Delta s(p) = s, \forall p \in \mathbf{P}$. $\Delta$ 保持有限极限, 这是因为 $\Delta$ 具有一个 left adjoint. $\alpha: S^{\mathbf{P}^{op}} \longrightarrow \mathrm{sh}(\mathbf{P}, \neg\neg)$ 是 sheafification 函子,

它将任一 presheaf 送到与其相应的 sheaf. $\alpha$ 为 left exact, 即保持有限极限. 特别乘积, monomorphism 都是不同类型的极限.

首先构造常量函子 $\Delta(B \times \mathbf{N}) = \Delta B \times \Delta\mathbf{N}$ 的一个子对象 $A$, $\forall p \in \mathbf{P}$, 定义 $A(p) = \{(b.n) \mid p(b,n) = 0\}$. 若 $q \leqslant p$, 则有 $A(q) \supseteq A(p)$.

**命题 7** 函子 $A$ 是 $\neg\neg$-closed 的, 即有 $\neg\neg A = A$.

$\Omega$ 是 $S^{\mathbf{P}^{op}}$ 中的 subobject classifier, $\Omega_{\neg\neg}$ 是 $\mathrm{sh}(\mathbf{P},\neg\neg)$ 中的 subobject classifier. 我们知道 $\Omega_{\neg\neg}$ 是 $1_\Omega$ : $\Omega \longrightarrow \Omega$ 以及 $\neg\neg$ : $\Omega \longrightarrow \Omega$ 的 equalizer. 由于 $\neg\neg A = A$, 所以 $A$ 的特征函数 $\Delta B \times \Delta\mathbf{N} \longrightarrow \Omega$ 分解于 $\Omega_{\neg\neg}$. 记这一分解为 $f$ : $\Delta B \times \Delta\mathbf{N} \longrightarrow \Omega_{\neg\neg}$. 它的 transpose 是 $g$ : $\Delta B \longrightarrow \Omega_{\neg\neg}^{\Delta N}$. 由于 $g$ 是 presheaf 的映射, monomorphism 可以逐点检验 (pointwise). 于是有以下引理.

**引理 1** $g$ 是一个 monomorphism.

由于 sheafification 函子保持 monomorphism, 所以 $\alpha(g)$ : $\alpha(\Delta B) \hookrightarrow \Omega_{\neg\neg}^{\alpha(\Delta\mathbf{N})}$ 也是一个 monomorphism. (可以证明 $\Omega_{\neg\neg}^{\alpha(\Delta\mathbf{N})} = \alpha(\Omega_{\neg\neg}^{\Delta\mathbf{N}})$). 我们记 $\alpha\Delta(\ )$ 为 $\widehat{(\ )}$, 则有 $\alpha(g)$ : $\widehat{B} \hookrightarrow \Omega_{\neg\neg}^{\widehat{\mathbf{N}}}$. 因为 Cohen topos $\mathrm{sh}(\mathbf{P},\neg\neg)$ 是布尔的, 所以 $\Omega_{\neg\neg} = 1 + 1 = \widehat{2}$, $\Omega_{\neg\neg}^{\widehat{\mathbf{N}}} = \widehat{2}^{\widehat{\mathbf{N}}}$. $\widehat{\mathbf{N}}$ 是 $\mathrm{sh}(\mathbf{P},\neg\neg)$ 的自然数对象. 这样 $\widehat{2}^{\widehat{\mathbf{N}}}$ 是自然数的 power set. 由 $S$ 中的 monomorphism $\mathbf{N} \hookrightarrow B$, 继而有 $\mathrm{sh}(\mathbf{P},\neg\neg)$ 中的 monomorphism $\widehat{\mathbf{N}} \hookrightarrow \widehat{B}$, 所以 $\widehat{\mathbf{N}} \hookrightarrow \widehat{B} \hookrightarrow \widehat{2}^{\widehat{\mathbf{N}}}$, 我们 "force" $\widehat{B}$ 于 $\widehat{2}^{\widehat{\mathbf{N}}}$ 内.

另一方面, 在集合的范畴 $S$ 中有基数关系 $\mathbf{N} < 2^{\mathbf{N}} < B$, 这一基数的严格不等关系, 可以证明在 Cohen topos 中同样成立, $\widehat{\mathbf{N}} < \widehat{2^{\mathbf{N}}} < \widehat{B}$. 这样就有 $\widehat{\mathbf{N}} < \widehat{2^{\mathbf{N}}} < \widehat{2}^{\widehat{\mathbf{N}}}$, $K = \widehat{2^{\mathbf{N}}}$ 正是我们需要的对象.

**定理 10** 在 Cohen topos $\mathrm{sh}(\mathbf{P},\neg\neg)$ 中选择公理成立, 而连续统假设不成立.

P. Freyd 构造了一个 sheaf topos $\mathrm{sh}(\mathbf{A},\neg\neg)$. 用它证明了选择公理独立于 ZF 的集合论公理. 这一证明的关键是构造一列 sheaf

$F_0, F_1, \cdots, F_n, \cdots$, 每一个都不空, 即 $F_n \longrightarrow 1$ 是一个 epimorphism, 但是它们的乘积 $\prod\limits_n F_n$ 却是空的, 即 $\prod\limits_n F_n$ 是 initial 对象. 这样选择公理不成立.

范畴 $\mathbf{A}$ 是如下构造的. 让 $\mathbf{N}$ 为自然数的集合, $\mathbf{A}$ 的对象是 $\mathbf{N}$ 的这样的有限子集 $n = \{0, 1, \cdots, n\}$, $n \in \mathbf{N}$. $\mathbf{A}$ 中的映射定义为

$$\mathbf{A}(n, m) = \begin{cases} \{n\text{在 } m \text{ 上的限制}\}, & \text{若 } m \leqslant n, \\ \phi, & \text{若 } m > n. \end{cases}$$

范畴 $\mathbf{A}$ 中的任一映射 $f: n \longrightarrow m$ 具有性质, 若有 $g \circ f = h \circ f$, 这里 $m \underset{h}{\overset{g}{\rightrightarrows}} k$, 那么 $g = h$, 即 $f$ 是 epimorphism.

**命题 8** sh$(\mathbf{A}, \neg\neg)$ 是二值的布尔 topos.

我们已经知道 sh$(\mathbf{A}, \neg\neg)$ 是布尔的. sh$(\mathbf{A}, \neg\neg)$ 的 terminal 对象 $1 = \mathbf{A}(_, 0)$, 而 $\mathbf{A}(_, 0)$ 只有 $\phi$ 以及其自身两个子 sheaf.

$\alpha: S^{\mathbf{A}^{op}} \longrightarrow$ sh$(\mathbf{A}, \neg\neg)$ 是 sheafification 函子. 定义 $F_n = \alpha(\mathbf{A}(_, n))$. 因为 $\mathbf{A}(_, n) \longrightarrow 1 = \mathbf{A}(_, 0)$ 是 epimorphism, 而 $\alpha$ 具有 right adjoint 且为 left exact, 这样 $F_n \longrightarrow 1$ 是 epimorphism. 对任意 $m \in \mathbf{N}$, 总存在 $n > m$, 这样 $\mathbf{A}(m, n) = \phi$, 于是 $\prod\limits_n \mathbf{A}(_, n)(m) = \prod\limits_n \mathbf{A}(m, n) = \phi$, 即 $\prod\limits_n \mathbf{A}(_, , n)$ 是 initial 对象. 同样可以证明 $\prod\limits_n F_n$ 是 sh$(\mathbf{A}, \neg\neg)$ 中的 initial 对象. 于是我们有以下定理.

**定理 11** 存在一个二值布尔 topos, 满足 ZF 公理, 但在其中选择公理不成立.

## §4 代数理论, 几何理论, 与分类 topos

1963 年 Lawvere 在他的博士论文中提出范畴化的代数理论以及函子化的模型论.

一个 (equational) 代数理论是一个小范畴 $\mathbf{A}$. $\mathbf{A}$ 的对象是自然数 $\{0,1,2,\cdots\}$, 或者等价地看为是由一个对象 $A$ 的有限乘积构成, $1=A^0$, $A=A^1, A^2, \cdots, A^n, \cdots$. 除了自然投影 $\pi_i^{(n)}: A^n \longrightarrow A$ 之外, $\mathbf{A}$ 中还有若干 $n$ 元运算 $A^n \longrightarrow A$. $n$ 元运算需要满足的方程 (如结合律, 可换律等) 由可换图形给出.

$C$ 是一个具有有限乘积的范畴. 代数理论 $\mathbf{A}$ 在 $C$ 中的一个模型 $F$ 是 $\mathbf{A}$ 到 $C$ 的一个保持有限乘积的函子, $F: \mathbf{A} \longrightarrow C$. $F(A^n)=F(A)^n$, 特别 $F(1)=1$. 作为函子 $F$ 是保持任一可换图形的. 两个模型之间的自然变换正是保持这一代数结构的同态. $\mathbf{A}$ 到 $C$ 的保持有限乘积的函子的全体, 以及它们之间的自然变换是函子范畴 $C^{\mathbf{A}}$ 的一个子范畴, 记为 $\mathrm{Mod}_C\mathbf{A}$ 或 $\mathrm{Alg}_C\mathbf{A}$.

例如群理论 $\mathbf{A}$ 具有一个 0 元运算 (单位元) $e: 1 \longrightarrow A$, 一个一元运算 (逆运算)$(\ )^{-1}: A \longrightarrow A$, 以及一个二元运算 $\cdot: A^2 = A\times A \longrightarrow A$.

二元运算满足结合律, 即以下图形可换.

$$\begin{array}{ccc} A\times A\times A & \xrightarrow{1_A\times\cdot} & A\times A \\ {\scriptstyle \cdot\times 1_A}\downarrow & & \downarrow{\scriptstyle \cdot} \\ A\times A & \xrightarrow[\cdot]{} & A \end{array}$$

单位元满足以下可换图形

$$\begin{array}{ccccc} A\approx A\times 1 & \xrightarrow{1_A\times e} & A\times A & \xleftarrow{e\times 1_A} & 1\times A\approx A \\ & {\scriptstyle 1_A}\searrow & \downarrow{\scriptstyle \cdot} & \swarrow{\scriptstyle 1_A} & \\ & & A & & \end{array}$$

逆运算满足以下可换图形

$$\begin{array}{ccccc} & (1_A,(\ )^{-1}) & & ((\ )^{-1},1_A) & \\ A & \longrightarrow & A\times A & \longleftarrow & A \\ \downarrow & & \downarrow\cdot & & \downarrow \\ 1 & \xrightarrow{e} & A & \xleftarrow{e} & 1 \end{array}$$

$F:\ \mathbf{A}\longrightarrow\mathcal{C}$ 是一个保持有限乘积的函子. 这样 $F(A)$ 是 $\mathcal{C}$ 中的一个群对象. 例如 $\mathcal{C}$ 是拓扑空间的范畴. 那么 $F(A)$ 是一个拓扑群. 若 $\mathcal{C}=\mathcal{S}$ 为集合的范畴, $F(A)$ 则是通常意义下的群.

若 $G$ 是另一个这样的函子. $F$ 到 $G$ 的一个自然变换 $\tau$ : $F\stackrel{\cdot}{\longrightarrow}G$ 是一个映射 $\tau_A$ : $F(A)\longrightarrow G(A)$. 并且满足

$$\tau_A(e)=e \qquad \begin{array}{ccc} 1 & \xrightarrow{0} & F(A) \\ & \searrow^{e} & \downarrow\tau_A \\ & & G(A) \end{array}$$

$$\tau_A(x,y)=\tau_A(x)\cdot\tau_A(y) \qquad \begin{array}{ccc} F(A)\times F(A) & \stackrel{\cdot}{\longrightarrow} & F(A) \\ \tau_A\times\tau_A\downarrow & & \downarrow\tau_A \\ G(A)\times G(A) & \stackrel{\cdot}{\longrightarrow} & G(A) \end{array}$$

这样 $\tau_A$ 是一个群同态.

一般代数结构有 monoid(有单位元的半群), 环, 环上的模, 格等等.

若代数理论 $\mathbf{D}$ 只有自然投影 $\pi_i^{(n)}$ : $D^n\longrightarrow D$, 那么一个 $\mathbf{D}$–模型即是一个集合. 这样 $\mathrm{Mod}\,\mathbf{D}=\mathcal{S}$. 我们称 $\mathbf{D}$ 为平凡代数理论.

两个代数理论 $\mathbf{A},\mathbf{B}$ 之间的映射是一个函子 $f$ : $\mathbf{B}\longrightarrow\mathbf{A}$. $f$ 诱导 $\mathbf{A}$– 模型到 $\mathbf{B}$– 模型的一个函子 $\mathrm{Mod}(f)$: $\mathrm{Mod}\,\mathbf{A}\longrightarrow\mathrm{Mod}\,\mathbf{B}$. 例如 $\mathbf{A}$ 为环的理论, $\mathbf{B}$ 为 monoid 理论, $\mathbf{B}$ 到 $\mathbf{A}$ 的嵌入 $i$ : $\mathbf{B}\longrightarrow\mathbf{A}$, monoid 二元运算对应于环乘法, $i$ 诱导环的范畴到 monoid 的范畴的 forgetful 函子. 又如平凡代数理论 $\mathbf{D}$ 到任一代数理论的嵌入 $u$ : $\mathbf{D}\longrightarrow\mathbf{A}$, 诱导一个 forgetful 函子 $\mathrm{Mod}\,u$ : $\mathrm{Mod}\,\mathbf{A}\longrightarrow\mathcal{S}$.

**定理 12**　函子 $\mathrm{Mod}(f): \mathrm{Mod}\,\mathbf{A} \longrightarrow \mathrm{Mod}\,\mathbf{B}$ 具有 adjoint.

这样由 monoid 理论 $\mathbf{B}$ 到环理论 $\mathbf{A}$ 的嵌入诱导的函子 $\mathrm{Mod}(i)$ 具有 left adjoint $\mathrm{Mod}\,\mathbf{B} \longrightarrow \mathrm{Mod}\,\mathbf{A}$, 称为 monoid ring; 而由平凡代数理论 $\mathbf{D}$ 到任一代数理论的嵌入诱导的 forgetful 函子具有 left adjoint, 这就是所谓自由结构，如自由群，自由 monoid 等.

代数理论的公理都是由方程式表示的. 而很多其它数学结构，如域，或代数几何里重要的局部环 (local ring) 的某些性质，却不能由方程式来描述. 如一个域是一个环，并且每一个非零元素都有逆元，这可以表示为

$$\forall x((x = 0) \vee \exists y(xy = 1)).$$

而局部环是一个环，并且还满足

$$\neg(0 = 1),$$
$$\exists y(xy = 1) \vee \exists z((1 - x)z = 1)$$

因而又有几何逻辑 (geometric logic).

一个几何理论的语言 $L$ 由以下成份组成.

1. 类型 (type) $X, Y, Z, \cdots$.

2. 函数符号 $f, g, \cdots$. 每一个函数符号结合有变量的类型 $(X_1, X_2, \cdots, X_n)$ 以及值的类型 $Y$.

3. 关系符号 $r, s, \cdots$. 每一关系符号结合有一列类型 $(X_1, X_2, \cdots, X_n)$, 它们是这一关系中所含变量的类型.

项 (term) 定义如下.

1. 对每一个类型 $X$, 变量 $x', x'', \cdots$ 均为项.

2. 函数 $f$ 具有变量类型 $X_1, X_2, \cdots, X_n$, 值类型 $Y$, 而 $t_1, t_2, \cdots, t_n$ 是分别具有类型 $X_1, X_2, \cdots, X_n$ 的项. 那么 $f(t_1, t_2, \cdots, t_n)$ 是类型为 $Y$ 的项.

公式 (formula) 定义如下.

1. $T$(真), $\perp$(假) 是公式.

2. 若 $s,t$ 是两个项, 那么 $s=t$ 是一个公式.

3. 若关系符号 $Y$ 结合有类型 $(X_1,X_2,\cdots,X_n)$, 而 $t_1,t_2,\cdots,t_n$ 分别为具有类型 $X_1,X_2,\cdots,X_n$ 的项, 那么 $Y(t_1,t_2,\cdots,t_n)$ 是一个公式.

4. 若 $\varphi,\psi$ 是公式, 那么 $\varphi\wedge\psi$, $\varphi\vee\psi$ 是公式.

5. $\varphi$ 是一个公式, $x$ 是一个变量, 那么 $\exists x\varphi$ 是一个公式.

一个相继式 (sequent) 具有如下形式 $\varphi\vdash\psi$, 这里 $\varphi,\psi$ 是公式. $\vdash$ 不是几何语言中的符号.

$L$ 是一个几何语言, $T$ 为一组相继式, $\mathbf{T}=(L,T)$ 是一个几何理论, $T$ 中的每一个相继式称为理论 $\mathbf{T}$ 的一个公理. 代数方程可以表示为相继式. 例如 $xy=yx$ 可以表示为 $T\vdash xy=yx$.

局部环的理论除了环的公理外还要求

$$0=1\vdash\perp,$$
$$T\vdash\exists x'(x\cdot x'=1)\vee\exists x''((1-x)x''=1).$$

$\mathcal{E}$ 是一个 topos, 几何语言 $L$ 在 $\mathcal{E}$ 中的一个解释 $I$ 使每一个类型 $X$ 对应于 $\mathcal{E}$ 中的一个对象 $X^{(I)}$; 函数符号 $f$ 具有变量类型 $(X_1,X_2,\cdots,X_n)$, 值的类型 $Y$ 对应于 $\mathcal{E}$ 中的映射 $f^{(I)}:\ X_1^{(I)}\times X_2^{(I)}\times\cdots\times X_n^{(I)}\longrightarrow Y^{(I)}$; 关系 $r$ 具有系列类型 $(X_1,X_2,\cdots,X_n)$ 对应于 $X_1^{(I)}\times X_2^{(I)}\times\cdots\times X_n^{(I)}$ 的一个子对象 $r^{(I)}\hookrightarrow X_1^{(I)}\times X_2^{(I)}\times\cdots\times X_n^{(I)}$. 特别记公式 $\varphi$ 所对应的子对象为 $\{x\mid\varphi(x)\}^{(I)}$, 变量 $x=(x_1,\cdots,x_k)$ 具有类型 $(X_1,\cdots,X_k)$.

一个相继式 $\varphi\vdash\psi$ 在解释 $I$ 下为真, 若有 $\{x\mid\varphi(x)\}^{(I)}\leqslant\{x\mid\psi(x)\}^{(I)}$ (这里需要适当增加 $\varphi$ 与 $\psi$ 所含的变量, 以求 $\varphi$ 和 $\psi$ 具有相同的变量).

一个解释 $I$ 称为理论 $\mathbf{T}$ 的一个模型, 若 $\mathbf{T}$ 中的每一公理在解释 $I$ 中为真.

语言 $L$ 的两个解释 $I, J$ 之间的一个映射 $\alpha: I \longrightarrow J$ 由一族映射组成，$\alpha_X: X^I \longrightarrow X^J$，这里 $X$ 是 $L$ 的类型. 对每一个函数 $f$，以下方形可换

$$\begin{array}{ccc} X_1^{(I)} \times X_2^{(I)} \times \cdots \times X_n^{(I)} & \xrightarrow{f^{(I)}} & Y^{(I)} \\ \downarrow \alpha_{x_1} \times \alpha_{x_2} \times \cdots \times \alpha_{x_n} & & \downarrow \alpha_Y \\ X_1^{(J)} \times X_2^{(J)} \times \cdots \times X_n^{(J)} & \xrightarrow{f^{(J)}} & Y^{(J)} \end{array}$$

对于每一个关系 $r$，存在映射 $\alpha_r: r^{(I)} \longrightarrow r^{(J)}$，使以下图形可换

$$\begin{array}{ccc} r^{(I)} & \longrightarrow & X_1^{(I)} \times X_2^{(I)} \times \cdots \times X_n^{(I)} \\ \downarrow \alpha_I & & \downarrow \alpha_{x_1} \times \alpha_{x_2} \times \cdots \times \alpha_{x_n} \\ r^{(J)} & \longrightarrow & X_1^{(J)} \times X_2^{(J)} \times \cdots \times X_n^{(J)} \end{array}$$

两个 $\mathbf{T}$ 模型之间的映射是它们作为语言 $L$ 的解释之间的映射. 这样语言 $L$ 在 $\mathcal{E}$ 中的解释以及解释之间的映射构成一个范畴 $\mathcal{E}_L$，而理论 $\mathbf{T}$ 的模型构成 $\mathcal{E}_L$ 的一个子范畴 $\mathrm{Mod}_{\mathcal{E}}\mathbf{T}$.

分类 (classifying)topos 的思想是，对一个几何理论 $\mathbf{T}$，结合有一个 $S$ (可以是其它 topos) 上的 topos $B(\mathbf{T})$，这样任一 topos $\mathcal{E}$ 中的 $\mathbf{T}$ 的模型的范畴 $\mathrm{Mod}_{\mathcal{E}}(\mathbf{T})$ 等价于 $\mathcal{E}$ 到 $B(\mathbf{T})$ 的几何映射的范畴 $\mathrm{Hom}(\mathcal{E}, B(\mathbf{T}))$. $\mathcal{E}$ 到 $B(\mathbf{T})$ 的一个几何映射

$$\mathcal{E} \underset{f_*}{\overset{f^*}{\rightleftarrows}} B(\mathbf{T}),$$

$f^*$ 正像代数理论中保持乘积的函子，$f^*$ 保持相应的几何结构. 给出 $\mathcal{E}$ 中的一个 $\mathbf{T}$ 模型.

这又像代数拓扑中分类空间 (classifying space) 的思想：$G$ 是一个可换群，对任一 $n$，存在一个拓扑空间 $K(G, n)$，若 $X$ 是

一个拓扑空间，$X$ 上的以 $G$ 为系数的 $n$ 维上同调 (cohomology) 群 $H^n(X,G)$ 一一对应于 $X$ 到 $K(G,n)$ 的连续映射的同伦类，$H^n(X,G)\approx[X,K(G,n)]$.

下面是两个分类 topos 的例子.

$\mathbf{Z}$ 是整数环. $\mathbf{Z}[x_1,\cdots,x_n]$ 是 $n$ 个变量的整系数多项式环. 一个 finitely presented 环具有形式 $\mathbf{Z}[x_1,\cdots,x_n]/(p_1,\cdots,p_k)$. 这里 $p_i$ 是 $\mathbf{Z}[x_1,\cdots,x_n]$ 中的多项式，$(p_1,\cdots,p_k)$ 是 $p_1,\cdots,p_k$ 生成的理想. 记 finitely presented 环以及它们之间的环同态构成的范畴为 $\mathrm{Alg}_{\mathbf{Z}}$. 张量积是 $\mathrm{Alg}_{\mathbf{Z}}$ 的 coproduct, 而商是 coequalizer. 这样，$\mathrm{Alg}_{\mathbf{Z}}$ 具有有限上极限 (colimit), 即它的对偶范畴 $\mathrm{Alg}_{\mathbf{Z}}^{op}$ 具有有限极限，并且 $\mathrm{Alg}_{\mathbf{Z}}^{op}$ 中的任一对象是由一元整系数多项式环 $\mathbf{Z}[x]$ 生成的，即利用张量积与商由 $\mathbf{Z}[x]$ 构造而成.

$F:\mathrm{Alg}_{\mathbf{Z}}^{op}\longrightarrow\mathcal{E}$ 是一个 left exact 函子 (保持有限极限). 那么 $F(\mathbf{Z}[x])$ 是 $\mathcal{E}$ 中的一个环. $\mathcal{E}$ 中环对象的范畴 $R(\mathcal{E})$ 等价于由 $\mathrm{Alg}_{\mathbf{Z}}^{op}$ 到 $\mathcal{E}$ 的 left exact 函子的范畴 $\mathrm{Lex}(\mathrm{Alg}_{\mathbf{Z}}^{op},\mathcal{E})$, 而 $\mathrm{Lex}(\mathrm{Alg}_{\mathbf{Z}}^{op},\mathcal{E})$ 等价于由 $\mathcal{E}$ 到 $S^{(\mathrm{Alg}_{\mathbf{Z}}^{op})^{op}}=S^{\mathrm{Alg}_{\mathbf{Z}}}$ 的几何映射的范畴 $\mathrm{Hom}(\mathcal{E},S^{\mathrm{Alg}_{\mathbf{Z}}})$. 于是有 $R(\mathcal{E})\approx\mathrm{Hom}(\mathcal{E},S^{\mathrm{Alg}_{\mathbf{Z}}})$. 这样 $S^{\mathrm{Alg}_{\mathbf{Z}}}$ 正是环理论所对应的分类 topos. 这一等价正是 $f\longmapsto f^*(\mathrm{Alg}_{\mathbf{Z}}(\mathbf{Z}[X],_))$, 因而称 $S^{\mathrm{Alg}_{\mathbf{Z}}}$ 中的环对象 $\mathrm{Alg}_{\mathbf{Z}}(\mathbf{Z}[X],_)$ 为 universal ring-object.

另一个例子是关于局部环的.

这里仍然取范畴 $\mathrm{Alg}_{\mathbf{Z}}^{op}$. 构造其上的 Grothendieck 拓扑 $J$. 对 $\mathrm{Alg}_{\mathbf{Z}}^{op}$ 的任一对象 $A$, 基复盖 (basic covering) 定义如下，$\{A\longrightarrow A[a_i^{-1}]\mid i=1,2,\cdots,n\}$, 这里 $a_1,\cdots,a_n$ 是 $A$ 中的元素，$(a_1,a_2,\cdots,a_n)$ 是 $a_1,a_2,\cdots,a_n$ 生成的理想，并且要求 $1\in(a_1,a_2,\cdots,a_n)$. 这样，$(\mathrm{Alg}_{\mathbf{Z}}^{op},J)$ 上的 sheaf 的 topos $\mathrm{sh}(\mathrm{Alg}_{\mathbf{Z}}^{op},J)$ 正是局部环的分类 topos. $\mathrm{sh}(\mathrm{Alg}_{\mathbf{Z}}^{op},J)$ 又称为 Zariski topos,

$$\mathrm{Hom}\big(\mathcal{E},\mathrm{sh}(\mathrm{Alg}_{\mathbf{Z}}^{op},J)\big)\approx\mathrm{LocRing}(\mathcal{E}).$$

给出一个几何理论 T, 有一般方法构造 $\mathbf{T}$ 的一个分类 topos. 首先构造 T 的一个 syntactic 范畴 $S(\mathbf{T})$. $S(\mathbf{T})$ 中的对象是 $\mathbf{T}$ 中公式的等价类，两个公式 $\varphi$ 与 $\psi$ 等价当且仅当对 T 的任一模型 $M$, $\{x \mid \varphi(x)\}^{(M)} = \{x \mid \psi(x)\}^{(M)}$. 记这一等价类为 $[\varphi, X]$. 这里 $X = (X_1, \cdots, X_n)$ 是 $\varphi$ 的变量的类型. $[\varphi, X]$ 到 $[\psi, Y]$ 的一个映射是另一个等价类 $[\sigma; X, Y]$, 这里 $\sigma$ 是一个公式，并且 $\{(x,y) \mid \sigma(x,y)\}^{(M)} \subseteq \{x \mid \varphi(x)\}^{(M)} \times \{y \mid \psi(y)\}^{(M)}$. 若 $[\sigma; X, Y]$ : $[\varphi, X] \longrightarrow [\psi, Y]$, $[\tau; Y, Z]$ : $[\psi, Y] \longrightarrow [\chi, Z]$, $[\sigma; X, Y]$ 与 $[\tau; Y, Z]$ 的复合是公式 $\exists y(\sigma(x,y) \wedge \tau(y,z))$.

不难检验, 如上定义的 $S(\mathbf{T})$ 构成一个范畴, 并且 $S(\mathbf{T})$ 具有有限极限. 可以定义 $S(\mathbf{T})$ 上的一个 Grothendieck 拓扑 $J$, $(S(\mathbf{T}), J)$ 上的 sheaf 的 topos $\mathrm{sh}(S(\mathbf{T}), J) = B(\mathbf{T})$ 正是理论 $\mathbf{T}$ 的分类 topos. 详细证明请见 [6].

## 参考文献


1 Johnston P T. Topos Theory. New York: Academic Press, 1977

2 Lambek J, Scott P J. Introduction to Higher Order Categorical Logic. Cambridge: Cambridge Univ. Press, 1986

3 Lawvere F W. Functorial semantics of algebraic theories. Proc. National Acad. Sci. U.S.A., 1963, 50: 869~872

4 Lawvere F W. An elementary theory of the category of sets. Proc. National Acad. Sci. U.S.A. 1964, 52: 1506~1511

5 Lawvere F W. Introduction to part I. Lecture Notes in Math., 1975, 445: 3~14

6 MacLane S, Moerdijk I. Sheaves in Geometry and Logic. Heidelberg: Spriger–Verlag, 1992

# 第 14 章

# 凸集范畴，enriched 范畴与度量空间范畴

凸集在统计决策论中有很重要的应用. 任意一个凸集可以嵌入一个 $K$- 模，凸集上定义有广义度量 dist, 因此一个凸集是一个度量空间. 在这一章里我们讨论凸集范畴 $\mathcal{C}$ 的性质，$\mathcal{C}$ 与 $K$- 模范畴 $K$-mod 的关系，$\mathcal{C}$ 与广义度量空间范畴 $\mathcal{U}$-Cat 的关系，enriched 范畴的概念，凸集范畴 $\mathcal{C}$ 是一个在 $\mathcal{U} = ([0,\infty], \geqslant)$ 中 enriched 范畴.

## §1　凸集范畴 $\mathcal{C}$ 与 $K$- 模范畴 $K$-mod

$K = \{r \in \mathbf{R} \mid r \geqslant 0\}$ 是非负实数构成的半环. 用 $K$-mod 表示 $K$- 模与 $K$- 模映射构成的范畴.

**定义 1**　$C$ 是一个集合，若对任意 $c_1, c_2 \in C$, $0 \leqslant t \leqslant 1$, $tc_1 + (1-t)c_2 \in C$, 那么 $C$ 是一个凸集. 若 $B$ 也是一个凸集，$C$ 到 $B$ 的一个凸映射 $f: C \longrightarrow B$ 是 $C$ 到 $B$ 的一个映射，并且保

持凸运算

$$f(tc_1+(1-t)c_2)=tf(c_1)+(1-t)f(c_2).$$

凸集与凸集之间凸映射构成范畴 $\mathcal{C}$

**命题 1** 范畴 $\mathcal{C}$ 具有卡氏积.

$C,B$ 是凸集. $C\times B$ 是 $C,B$ 作为集合的卡氏积. $(c_1,b_1)$, $(c_2,b_2)\in C\times B$,

$$t(c_1,b_1)+(1-t)(c_2,b_2)=(tc_1+(1-t)c_2,tb_1+(1-t)b_2).$$

让 $P_C,P_B$ 分别为 $C\times B$ 到 $C,B$ 的投影, $(C\times B,P_C,P_B)$ 具有性质: 对一对凸映射 $f: D\longrightarrow C$, $g: D\longrightarrow B$. 存在唯一凸映射 $(f,g): D\longrightarrow C\times B$, 并且 $P_C\circ(f,g)=f$, $P_B\circ(f,g)=g$.

**定义 2** $C,B$ 和 $D$ 是凸集. $C\times B$ 到 $D$ 的一个映射 $f$: $C\times B\longrightarrow D$ 称为双凸映射, 若 $f$ 对两个分量分别是凸映射.

**定义 3** $C,B$ 是两个凸集. $C$ 与 $B$ 的张量积 $C\otimes B$ 是范畴 $\mathcal{C}$ 中的一个对象, 且有双凸映射 $i$: $C\times B\longrightarrow C\otimes B$, 具有性质: 对于任意凸集 $D$, 以及双凸映射 $f$: $C\times B\longrightarrow D$, 存在唯一凸映射 $\overline{f}$: $C\otimes B\longrightarrow D$. 使得 $\overline{f}\circ i=f$.

$$\begin{array}{ccc} C\times B & \xrightarrow{i} & C\otimes B \\ & f\searrow \quad \swarrow\overline{f} & \\ & D & \end{array}$$

**定理 1** $C,B$ 是凸集, $C$ 和 $B$ 的张量积在 $\mathcal{C}$ 中存在.

**证明** 让 $F(C\times B)$ 为 $C\times B$ 生成的自由凸集. 在 $F(C\times B)$ 上定义一个由以下关系生成的同余二元关系 $\sim$:

$$0\leqslant t_i\leqslant 1,\ \sum_{i=1}^{n}t_i=1;\ 0\leqslant s_j\leqslant 1,\ \sum_{j=1}^{m}s_j=1,$$

$$\left(\sum_{i=1}^{n} t_i c_i, b\right) \sim \sum_{i=1}^{n} t_i(c_i, b);\ \left(c, \sum_{j=1}^{m} s_j b_j\right) \sim \sum_{j=1}^{m} s_j(c, b_j),$$

这样，$F(C\times B)/\sim$ 是一个凸集. 用 $c\otimes b$ 表示 $(c,b)$ 所在的同余类. 我们要证明 $F(C\times B)/\sim$ 是 $C$ 和 $B$ 的张量积.

首先有双凸映射 $i:\ C\times B\longrightarrow F(C\times B)/\sim$, $i(c,b)=c\otimes b$. 若 $f:\ C\times B\longrightarrow D$ 是一个双凸映射，因为 $F(C\times B)$ 是 $C\times B$ 生成的自由凸集，这样就有 $F(C\times B)$ 到 $D$ 的凸映射 $\widehat{f}:\ F(C\times B)\longrightarrow D$, 因为 $f$ 是双凸的. 所以 $\widehat{f}$ 将 $F(C\times B)$ 中位于相同同余类的元素送到 $D$ 中的同一元素. 这样 $\widehat{f}$ 诱导一个凸映射 $\overline{f}:\ F(C\times B)/\sim\longrightarrow D$, 并且 $\overline{f}\circ i=f$. 若 $g$ 是另一凸映射 $g:\ F(C\times B)/\sim\longrightarrow D$. 并且满足 $g\circ i=f$. 那么对于 $c\in C, b\in B$,

$$\begin{array}{ccc} C\times B & \longrightarrow & F(C\times B) \\ f\downarrow & \widehat{f}\swarrow & \downarrow \\ D & \xleftarrow[\overline{f}]{} & F(C\times B)/\sim \end{array}$$

$$g(c\otimes b)=g\circ i(c,b)=f(c,b)=\overline{f}\circ i(c,b)=\overline{f}(c\otimes b).$$

这证明了 $\overline{f}$ 的唯一性.

我们将 $C$ 与 $B$ 的张量积 $F(C\times B)/\sim$ 表示为 $C\otimes B$.

**命题 2** 若 $f:\ C\longrightarrow C'$, $g:\ B\longrightarrow B'$ 是两个凸映射. 定义 $f\otimes g(c,b)=f(c)\otimes g(b)$. 这样 $f\otimes g$ 可以唯一地扩张为从 $C\otimes B$ 到 $C'\otimes B'$ 的一个凸映射.

**证明** 这是因为 $\{c\otimes b\mid c\in C, b\in B\}$ 是 $C\otimes B$ 的生成元，并且 $f,g$ 是凸映射.

**推论** $\otimes:\ \mathcal{C}\times\mathcal{C}\longrightarrow\mathcal{C}$ 是一个双函子 (bifunctor).

**命题 3** $C,B$ 是凸集. $C$ 到 $B$ 的凸映射的集合 $\mathcal{C}(C,B)$ 也是一个凸集.

**定理 2** 对任意三个凸集 $C,B,D$ 存在自然同构

$$\varphi_{CBD}:\ \mathcal{C}(C\otimes B, D)\approx\mathcal{C}(C,\mathcal{C}(B,D)).$$

**证明** $f: C\otimes B \longrightarrow D$ 为一凸映射. 定义

$$\varphi_{CBD}(f)=\overline{f}:\ C\longrightarrow \mathcal{C}(B,D),\quad \overline{f}(c)(b)=f(c\otimes b)$$

(1) $\overline{f}(c)$ 是凸映射: $b_i\in B, 0\leqslant t_i\leqslant 1, \sum\limits_{i=1}^{n} t_i=1$.

$$\begin{aligned}\overline{f}(c)\left(\sum_{i=1}^{n} t_ib_i\right)&=f\left(c\otimes\sum_{i=1}^{n} t_ib_i\right)=f\left(\sum_{i=1}^{n} t_ic\otimes b_i\right)\\&=\sum_{i=1}^{n} t_if(c\otimes b_i)=\sum_{i=1}^{n} t_i\overline{f}(c)(b_i)\end{aligned}$$

(2) $\overline{f}:\ C\longrightarrow \mathcal{C}(B,D)$ 是凸映射

$$\begin{aligned}\overline{f}\left(\sum_{i=1}^{n} t_ic_i\right)(b)&=f\left(\left(\sum_{i=1}^{n} t_ic_i\right)\otimes b\right)=f\left(\sum_{i=1}^{n} t_i(c_i\otimes b)\right)\\&=\sum_{i=1}^{n} t_if(c_i\otimes b)=\sum_{i=1}^{n} t_i\overline{f}(c_i)(b)\end{aligned}$$

(3) $\varphi_{CBD}$ 是一一的

若有 $\overline{f}_1=\overline{f}_2$, 对 $c\in C$, $b\in B$, $\overline{f}_1(c)(b)=\overline{f}_2(c)(b)$. 但这正是 $f_1(c\otimes b)=f_2(c\otimes b)$, 即有 $f_1=f_2$.

(4) $\varphi_{CBD}$ 是到上的.

$g:\ C\longrightarrow \mathcal{C}(B,D)$ 是一个凸映射. 定义 $\widehat{g}:\ C\otimes B\longrightarrow D$, $\widehat{g}\left(\sum\limits_{i=1}^{n} t_ic_i\otimes b_i\right)=\sum\limits_{i=1}^{n} t_ig(c_i)(b_i)$. $\widehat{g}$ 是凸映射. $\overline{\widehat{g}}:\ C\longrightarrow \mathcal{C}(B,D)$, $\overline{\widehat{g}}(c)(b)=\widehat{g}(c\otimes b)=g(c)(b)$. 所以 $\overline{\widehat{g}}=g$.

**推论** $C$ 是一个闭合的 (closed) 范畴.

非负实数 $K$ 构成一个半环. 用 $K$-mod 表示 $K$- 模的范畴.

注意, 并不是每一个 $K$- 模都可以嵌入一个 $\mathbf{R}$- 模 ($\mathbf{R}$ 是实数域). 例如由两个元素 $\{l,h\}$ 如下生成的 $K$- 模 $M$, 这里 $l$ 代表轻,

$h$ 代表重. 对于 $r, s \in K$, $s \neq 0$, $rl + sh = sh$. $K$- 模 $M$ 并不能嵌入任何一个 $\mathbf{R}$- 模.

每一个 $K$- 模都是一个凸集, 每一个 $K$- 模映射都是一个凸映射. 所以有 underlying 函子 $u_0$ : $K$-mod$\longrightarrow C$. 下面我们要证明任一凸集都可以嵌入一个 $K$- 模.

$C$ 是一个凸集. 若 $C$ 是空集 $\phi$, 让 $F_0(C) = \{0\}$ 为一个元素的凸集.

若 $C \neq \phi$, 在 $C \times K$ 上定义一个二元关系

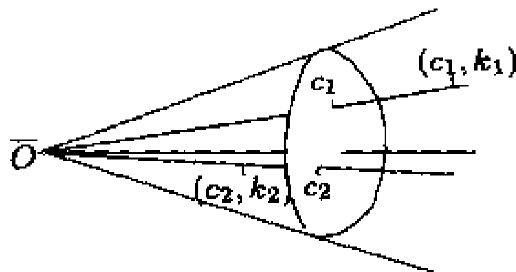
$(c_1, k_1) \sim (c_2, k_2)$ 当且仅当 1) $c_1 = c_2$, $k_1 = k_2$, 或 2) $k_1 = k_2 = 0$.

易见, 这是一个等价关系.

让 $F_0(C) = C \times K/\sim$. 在 $F_0(C)$ 上定义以下运算

$$
\begin{aligned}
&r, k \in K,\ c \in C,\ r(c, k) = (c, rk);\\
&k_1, k_2 \in K, k_1 \neq 0, \text{ 或 } k_2 \neq 0,\ c_1, c_2 \in C\\
&(c_1, k_1) + (c_2, k_2) = \left(\frac{k_1 c_1 + k_2 c_2}{k_1 + k_2}, k_1 + k_2\right)\\
&\bar{0} + \bar{0} = \bar{0}, \text{ 这里 } \bar{0} \text{ 是 } (c, 0) \text{ 的等价类}
\end{aligned}
$$

可以检验以上定义在等价类代表上的数乘和加法运算确是等价类的运算, 并且在这些运算下, $C \times K/\sim$ 构成一个 $K$- 模. 如下图, $C \times K/\sim$ 是凸集 $C$ 生成的锥, 见 [4].



若 $f: C \longrightarrow B$ 是一个凸映射. 定义

$$F_0(f) = \overline{f}: C \times K/\sim \longrightarrow B \times K/\sim, \ \overline{f}(c,k) = (f(c),k).$$

$$\overline{f}(r(c,k)) = \overline{f}(c,rk) = (f(c),rk) = r(f(c),k) = r\overline{f}(c,k);$$

$$\begin{aligned}
\overline{f}((c_1,k_1)+(c_2,k_2)) &= \overline{f}\left(\frac{k_1c_1+k_2c_2}{k_1+k_2}, k_1+k_2\right) \\
&= \left(f\left(\frac{k_1c_1+k_2c_2}{k_1+k_2}\right), k_1+k_2\right) \\
&= \left(\frac{k_1}{k_1+k_2}f(c_1)+\frac{k_2}{k_1+k_2}f(c_2), k_1+k_2\right) \\
&= (f(c_1),k_1)+(f(c_2),k_2) \\
&= \overline{f}(c_1,k_1)+\overline{f}(c_2,k_2).
\end{aligned}$$

这样, $F_0(f) = \overline{f}$ 是一个 $K$- 模映射.

**定理 3** $K$-mod $\underset{u_0}{\overset{F_0}{\leftrightarrows}}$ $C$, $F_0$ 是 $u_0$ 的 left adjoint.

证明见 [3].

$M, N$ 是 $K$- 模, $h: M \longrightarrow K, g: N \longrightarrow K$ 是 $K$- 模映射. 这样 $h, g$ 是范畴 $K$-mod$/K$ 中的对象. $h$ 到 $g$ 的一个映射是 $M$ 到 $N$ 的一个映射 $f: M \longrightarrow N$, 并且满足 $h = g \circ f$.

$$\begin{array}{ccc}
M & \xrightarrow{f} & N \\
& {}_{h}\searrow \quad \swarrow_{g} & \\
& K &
\end{array}$$

对于 $h: M \longrightarrow K$, $h^{-1}(1) = \{m \in M \mid h(m) = 1\}$ 是一个凸集. $f$ 诱导 $h^{-1}(1)$ 到 $g^{-1}(1)$ 的一个凸映射 $f|_{h^{-1}(1)}: h^{-1}(1) \longrightarrow g^{-1}(1)$. 由于 $g \circ f = h$.

若 $g^{-1}(1) = \phi$, 那么 $h^{-1}(1) = \phi$;

若 $h^{-1}(1) = \phi$, 那么 $f|_{h^{-1}(1)}$ 正是空集 $\phi$ 到 $g^{-1}(1)$ 的唯一嵌入. 若 $h^{-1}(1) \neq \phi$, $m \in h^{-1}(1)$,

$1 = h(m) = g \circ f(m) = g(f(m))$, 所以 $f(m) \in g^{-1}(1)$.

这样我们得到 $K$-mod$/K$ 到 $\mathcal{C}$ 的一个函子

$$G: K\text{-mod}/K \longrightarrow \mathcal{C},$$

$$G\left(\begin{array}{c} M \\ \downarrow h \\ K \end{array}\right) = h^{-1}(1), \quad G(f) = f|_{h^{-1}(1)}.$$

我们要证明函子 $G$ 有一个 left adjoint $F: \mathcal{C} \longrightarrow K$-mod$/K$. 这是以下这个一般定理的一种特殊情况.

**定理 4** $\mathcal{B}, \mathcal{E}$ 是两个范畴, $\mathcal{B}$ 具有 pullback. 若有函子对 $F_0, G_0$, $\mathcal{B} \underset{G_0}{\overset{F_0}{\rightleftarrows}} \mathcal{E}$, $F_0$ 是 $G_0$ 的 left adjoint, 那么对 $\mathcal{B}$ 中任意对象 $B$, 有两个函子 $\mathcal{B}/B \underset{G}{\overset{F}{\rightleftarrows}} \mathcal{E}/F_0(B)$, 并且 $F$ 是 $G$ 的 left adjoint.

**证明** 定义 $F\left(\begin{array}{c} X \\ \downarrow h \\ B \end{array}\right) = \begin{array}{c} F_0(X) \\ \downarrow F(h) \\ F_0(B) \end{array}$. 对于 $\begin{array}{c} E \\ \downarrow g \\ F_0(B) \end{array} \in \mathcal{E}/F_0(B)$, 构造以下 pullback(在 $\mathcal{B}$ 中),

$$\begin{array}{ccc} P(B) & \xrightarrow{\pi} & G_0(E) \\ {\scriptstyle \widehat{g}}\downarrow & & \downarrow {\scriptstyle G_0(g)} \\ B & \xrightarrow{\eta_B^0} & G_0F_0(B) \end{array}$$

这里 $\eta_B^0$ 是 adjoint 函子对 $F_0, G_0$ 的 unit.

定义 $G\left(\begin{array}{c} E \\ \downarrow g \\ F_0(B) \end{array}\right) = \begin{array}{c} P(B) \\ \downarrow \widehat{g} \\ B \end{array}$. 立即可见, $F, G$ 均为函子. 要证 $F$ 是 $G$ 的 left adjoint, 我们构造 $\mathcal{E}/F_0(B)\left(F\left(\begin{array}{c} X \\ \downarrow h \\ B \end{array}\right), \begin{array}{c} E \\ \downarrow g \\ F_0(B) \end{array}\right)$

与 $B/B\left(\begin{array}{c}X\\ \downarrow h\\ B\end{array}, G\left(\begin{array}{c}E\\ \downarrow g\\ F_0(B)\end{array}\right)\right)$ 之间的一个自然同构 $\alpha$.

若 $f:\ \begin{array}{c}F_0(X)\\ \downarrow F_0(h)\\ F_0(B)\end{array} \longrightarrow \begin{array}{c}E\\ \downarrow g\\ F_0(B)\end{array}$, 即有 $F_0(h)=g\circ f$. 在以下的 pullback 图形中

$$\begin{array}{ccccc}
X & & \xrightarrow{\eta_X^0} & & G_0F_0(X)\\
 & \searrow \overline{f} & & & \downarrow G_0(f)\\
 & & P(E) & \xrightarrow{\pi} & G_0(E)\\
 & h \searrow & \downarrow \widehat{g} & & \downarrow G_0(g)\\
 & & B & \xrightarrow{\eta_B^0} & G_0F_0(B)
\end{array}$$

$$\begin{aligned}G_0(g)\circ G_0(f)\circ\eta_X^0 &= G_0(g\circ f)\circ\eta_X^0\\ &= G_0F_0(h)\circ\eta_X^0=\eta_B^0\circ h.\end{aligned}$$

所以存在唯一 $\overline{f}: X\longrightarrow P(E)$, 使得 $\widehat{g}\circ\overline{f}=h$. 定义 $\alpha(f)=\overline{f}$.

反之, 若 $\overline{f}:\ \begin{array}{c}X\\ \downarrow h\\ B\end{array} \longrightarrow G\left(\begin{array}{c}E\\ \downarrow g\\ F_0(B)\end{array}\right) = \begin{array}{c}P(E)\\ \downarrow \widehat{g}\\ B\end{array}$, 即有 $h=\widehat{g}\circ\overline{f}$.

定义 $\beta(\overline{f}):\ \begin{array}{c}F_0(X)\\ \downarrow F_0(h)\\ F_0(B)\end{array} \longrightarrow \begin{array}{c}E\\ \downarrow g\\ F_0(B)\end{array}$ 为 $X\xrightarrow{\overline{f}} P(E)\xrightarrow{\pi} G_0(E)$ 的 transpose, 即 $\beta(\overline{f})=\varepsilon_E^0\circ F_0(\pi\circ\overline{f})$.

$$\begin{array}{ccccccc}
F_0(X) & \xrightarrow{F_0(\overline{f})} & F_0P(E) & \xrightarrow{F_0(\pi)} & F_0G_0(E) & \xrightarrow{\varepsilon_E^0} & E\\
 & \searrow F_0(h) & \downarrow F_0(\widehat{g}) & & \downarrow F_0G_0(g) & & \downarrow g\\
 & & F_0(B) & \xrightarrow[F_0(\eta_B^0)]{} & F_0G_0F_0(B) & \xrightarrow[\varepsilon_{F_0(B)}^0]{} & F_0(B)
\end{array}$$

因为 $\mathcal{E}^0_{F_0(B)} \circ F_0(\eta^0_B) = 1_{F_0(B)}$, 所以

$$\begin{aligned} g \circ \beta(\overline{f}) &= g \circ \mathcal{E}^0_E \circ F_0(\pi) \circ F_0(\overline{f}) \\ &= \mathcal{E}^0_{F_0(B)} \circ F_0 G_0(g) \circ F_0(\pi) \circ F_0(\overline{f}) \\ &= \mathcal{E}^0_{F_0(B)} \circ F_0(\eta^0_B) \circ F_0(\widehat{g}) \circ F_0(\overline{f}) \\ &= 1_{F_0(B)} \circ F_0(\widehat{g} \circ \overline{f}) \\ &= F_0(h). \end{aligned}$$

通过同样的 diagram chasing 和计算, 可以检验, $\beta$ 是 $\alpha$ 的逆; 并且 $\alpha$ 与 $\beta$ 都是自然的.

回到凸集范畴 $\mathcal{C}$ 与 $K$- 模范畴 $K$-mod.

$$G: K\text{-mod}/K \longrightarrow \mathcal{C},\ G\left(\begin{array}{c} M \\ \downarrow h \\ K \end{array}\right) = h^{-1}(1),\ G(f) = f|_{h^{-1}(1)}.$$

**推论** $G$ 具有 left adjoint $F$.

**证明** 在以上定理 4 中, 让 $\mathcal{B} = \mathcal{C}$, $B = 1$ 为一个元素的凸集, 这样 $\mathcal{C}/1 \approx \mathcal{C}$; 让 $\mathcal{E} = K$-mod, $F_0 = F_0$, $G_0 = u_0$. 那么 $F_0(1) = K$ 是一个生成元的自由 $K$- 模, $C$ 是一个凸集. $C \approx (C \longrightarrow 1)$. $F(C) = F(C \longrightarrow 1) = (F_0(C) \longrightarrow F_0(1)) = (C \times K/\sim \xrightarrow{P_c} K)$, 因为 $C \longrightarrow 1$ 将 $C$ 中的元素都送到一个生成元的自由凸集 $K$ 的唯一生成元, 所以 $P_c(c,k) = k$.

对于 $\begin{array}{c} M \\ \downarrow h \\ K \end{array} \in K\text{-mod}/K$, 在范畴 $\mathcal{C}$ 中的 pullback 图形中

$$\begin{array}{ccc} P(M) & \longrightarrow & u_0(M) \\ \Big\downarrow & & \Big\downarrow u_0(h) \\ 1 & \xrightarrow{\eta^0_1} & u_0(K) \end{array}$$

因为 $u_0(K) = u_0F_0(1) = K$, $\eta_1^0(1) = 1$, 所以 pullback $P(M) = h^{-1}(1)$. 即有 $G\left(\begin{array}{c} M \\ \downarrow h \\ K \end{array}\right) = h^{-1}(1)$

$$C \underset{G}{\overset{F}{\rightleftarrows}} K\text{-mod}/K$$

由定理 4, $F$ 是 $G$ 的 left adjoint.

**命题 4** 若 $C$ 是一个凸集, 那么 $C \approx GF(C)$. 若 $C \neq \phi$, 那么 $GF(C) = G\left(\begin{array}{c} C \times K/\sim \\ \downarrow P_c \\ K \end{array}\right) = P_c^{-1}(1) = \{(c,1) \mid c \in C\}$.

这样 $C \longrightarrow GF(C)$, $c \longmapsto (c,1)$ 是 $C$ 中的一个同构.

若 $C = \phi$, $GF(\phi) = G\left(\begin{array}{c} \{0\} \\ \downarrow 0 \\ K \end{array}\right) = \phi$.

**推论** 凸集的范畴 $C$ 等价于 $K$–mod$/K$ 的一个 coreflexive 子范畴.

**命题 5** $\begin{array}{c} M \\ \downarrow h \\ K \end{array} \in K\text{-mod}/K$, 那么 $FG\left(\begin{array}{c} M \\ \downarrow h \\ K \end{array}\right) \approx \begin{array}{c} M \\ \downarrow h \\ K \end{array}$ 当且仅当 $h^{-1}(0) \approx \{0\}$.

**证明** $FG\left(\begin{array}{c} M \\ \downarrow h \\ K \end{array}\right) = \begin{array}{c} h^{-1}(1) \times K/\sim \\ P_{h^{-1}(1)} \downarrow \\ K \end{array}$. 若 $FG\left(\begin{array}{c} M \\ \downarrow h \\ K \end{array}\right) \approx \begin{array}{c} M \\ \downarrow h \\ K \end{array}$, 则存在 $K$- 模同构 $f: h^{-1}(1) \times K/\sim \longrightarrow M$, 并且 $P_{h^{-1}(1)} = h \circ f$, 或 $P_{h^{-1}(1)} \circ f^{-1} = h$. 因为 $\ker P_{h^{-1}(1)} = \bar{0}$, 而 $f^{-1}$ 是同构, 所以 $h$ 的核 (kernel) 是 $\{0\}$.

反之，若 $h^{-1}(0)=\{0\}$, 我们定义

$$\begin{aligned}&g:\ M\longrightarrow h^{-1}(1)\times K/\sim,\\ &\quad g(m)=\left(\frac{m}{h(m)},h(m)\right)\quad 若\ m\neq 0,\\ &\quad g(0)=\overline{0}.\end{aligned}$$

由直接计算可知，$g$ 是一个 $K$- 模同态，$P_{h^{-1}(1)}\circ g=h$, $g$ 是到上的，一一的，因而 $g$ 是 $FG\left(\begin{array}{c}M\\ \downarrow h\\ K\end{array}\right)$ 到 $\begin{array}{c}M\\ \downarrow h\\ K\end{array}$ 的一个同构.

**定理 5** 函子 $F:\ C\longrightarrow K\text{-mod}/K$ 具有 left adjoint $L:\ K\text{-mod}/K\longrightarrow C$.

**证明** 函子 $L$ 的构造如下：$\begin{array}{c}M\\ \downarrow h\\ K\end{array}\in K\text{-mod}/K$, 因为 $h^{-1}(0)$ 是 $M$ 的一个子模，构造商模 $M/h^{-1}(0)$. 这样有 $M/h^{-1}(0)$ 到 $K$ 的 $K$- 模映射 $\overline{h}:\ M/h^{-1}(0)\longrightarrow K$, $\overline{h}(\overline{m})=h(m)$, 并且以下三角形可换

$$\begin{array}{ccc}M & \longrightarrow & M/h^{-1}(0)\\ & {\scriptstyle h}\searrow \quad \swarrow{\scriptstyle \overline{h}} & \\ & K & \end{array}$$

若 $g$ 是从 $\begin{array}{c}M\\ \downarrow h\\ K\end{array}$ 到 $\begin{array}{c}M'\\ \downarrow h'\\ K\end{array}$ 的一个 $K$- 模同态，即 $h=h'\circ g$. 那么 $g$ 诱导一个 $K$- 模同态

$$\widetilde{g}:\ M/h^{-1}(0)\longrightarrow M'/h'^{-1}(0),\ \widetilde{g}(\overline{m})=\overline{g(m)}.$$

定义 $L\left(\begin{array}{c}M\\ \downarrow h\\ K\end{array}\right)=\overline{h}^{-1}(1)$, $L(g)=\widetilde{g}|_{\overline{h}^{-1}(1)}$.

由直接计算可以验证：$L$ 是一个函子，$L$ 是 $F$ 的 left adjoint.

## §2 Enriched 范畴与广义度量空间范畴

一种数学结构与它们之间保持此种结构的映射构成一个范畴. 很多时候，保持结构的映射本身也具有某种结构，并且这种结构的范畴是闭合的 (closed). 例如两个 poset 之间的保序映射也是一个 poset, poset 的范畴是卡氏积闭合的 (注意， poset 不是偏序集！poset 是 pre–ordered set, 二元关系 "$\leqslant$" 要求满足以下两条： 1) $x \leqslant x$, 2) $x \leqslant y$ 和 $y \leqslant z \Longrightarrow x \leqslant z$; 偏序集 (partial ordered set) 还要求反对称性 $x \leqslant y$ 和 $y \leqslant x \Longrightarrow x = y$). $R$ 是一个可换环. 两个 $R$- 模之间的 $R$- 模同态的集合也是一个 $R$- 模. 而 $R$- 模的范畴 $R$–mod 也是闭合的 (但不是卡氏积闭合的), 我们刚看到两个凸集之间的凸映射的集合也是一个凸集. 凸集的范畴 $C$ 是闭合的.

Enriched 范畴最早是纯技术地用来研究本身很复杂的一些数学结构. 如 compactly generated topological spaces, Banach spaces, differential graded modules 等等. 它的技术性很强，常常使初学者望而生畏.

Lawvere 认为 enriched 范畴论是方法论的一部分，它有利于我们看到表面不同概念之间的内在联系，便于我们认识事物的特殊性与普遍性之间的联系. 他将 enriched 范畴理论用到简单数学结构如度量空间， poset 上，使得可以从范畴论的角度得到有关度量空间和逻辑的一般结论. 这使得 enriched 范畴论变得简单而又富有启发性. [2]

首先我们讨论具有张量积的范畴，即 monoidal 范畴.

**定义 4** 一个 monoidal 范畴 $\mathcal{U}$ 具有一个张量积 $\otimes : \mathcal{U}\times\mathcal{U} \longrightarrow \mathcal{U}$. 张量积 $\otimes$ 是一个函子，它具有单位 $I$, $I$ 是 $\mathcal{U}$ 中一个对象，并

且具有三个自然同构

$$a_{XYZ}: (X\otimes Y)\otimes Z \xrightarrow{\sim} X\otimes(Y\otimes Z),$$
$$l_X: I\otimes X \xrightarrow{\sim} X,$$
$$r_X: X\otimes I \xrightarrow{\sim} X,$$

使得以下两个图形可换.

$$\begin{array}{ccccc} ((W\otimes X)\otimes Y)\otimes Z & \xrightarrow{a\otimes 1} & (W\otimes(X\otimes Y))\otimes Z & \xrightarrow{a} & W\otimes((X\otimes Y)\otimes Z) \\ \downarrow a & & & & \downarrow 1\otimes a \\ (W\otimes X)\otimes(Y\otimes Z) & & \xrightarrow{a} & & W\otimes(X\otimes(Y\otimes Z)) \end{array}$$

$$\begin{array}{ccc} (X\otimes I)\otimes Y & \xrightarrow{a} & X\otimes(I\otimes Y) \\ & r\otimes 1 \searrow \quad \swarrow 1\otimes l & \\ & X\otimes Y & \end{array}$$

若将张量积 $\otimes$ 看为范畴 $\mathcal{U}$ 中对象上的二元运算, 同构作为相等关系, 那么这个二元运算是可结合的, 并且有单位元, 因而构成一个 monoid. 我们用 $(\mathcal{U},\otimes,I)$ 表示这个 monoidal 范畴.

任一具有卡氏积的范畴是一个 monoidal 范畴, 卡氏积就是张量积. 例如, 集合的范畴 $\mathcal{S}$, 范畴的范畴 Cat, 拓朴空间的范畴 Top 等等. 一个 poset$(P,\leqslant)$ 作为一个范畴, 任意两个元素之间最多只有一个映射, $P(a,b)\neq\phi$ 当且仅当 $a\leqslant b$. 合取 (conjunction) $\wedge$ 即是 $P$ 的卡氏积, 最大元 1 是合取的单位, 以上 monoidal 范畴的两个可换图形自然满足. 最简单的 poset $\mathbf{2}=\{0,1\}$, $0\leqslant 1$, 是经典逻辑的真值集.

$R$- 模的范畴具有张量积, 即通常的 $R$- 模张量积, 环 $R$ 是这一张量积的单位. $R$-mod 是一个 monoidal 范畴. 凸集的范畴 $\mathcal{C}$ 也是一个 monoadal 范畴.

让 $[0,\infty]$ 作为扩张了的非负实数, $\mathcal{U}=([0,\infty],\geqslant)$ 是一个 poset. 加法成为 $\mathcal{U}$ 的一个张量积. 0 是单位.

**定义 5** 一个 monoidal 范畴 $(\mathcal{U}, \otimes, I)$ 称为闭合的，若张量积 $\otimes$ 具有 right adjoint Hom: $\mathcal{U} \longrightarrow \mathcal{U}$,

$$\frac{A \otimes B \longrightarrow C}{A \longrightarrow \mathrm{Hom}(B, C)}, \qquad \frac{A \otimes B \longrightarrow C}{B \longrightarrow \mathrm{Hom}(A, C)}.$$

若张量积是卡氏积，这个 right adjoint $\mathrm{Hom}(B, C)$ 常记为 $C^B$，称为由 $B$ 到 $C$ 的函数空间．例如集合的范畴 $\mathcal{S}$, $C^B$ 是 $B$ 到 $C$ 的映射的集合；范畴的范畴 Cat, $C^B$ 是 $B$ 到 $C$ 的函子的集合．拓扑空间的范畴 Top 不是卡氏积闭合的，这是因为没有一个一般的方法定义一个函数空间上的拓扑．

一个 poset $P$ 是卡氏积闭合的，当且仅当 $P$ 是一个 Heyting 代数， Heyting operation$\longrightarrow$ 是合取 $\wedge$ 的 right adjoint,

$$\frac{a \wedge b \leqslant c}{a \leqslant b \longrightarrow c}.$$

例如 $P$ 是集合 $X$ 的子集的集合， $P = (2^X, \subseteq)$ 是一个 Heyting 代数． $B, C \in 2^X$, $B \longrightarrow C = C \cup (X \setminus B)$, 则有

$$\frac{A \cap B \subseteq C}{A \subseteq B \longrightarrow C}.$$

$\mathcal{U} = ([0, \infty], \geqslant)$ 是 monoidal 闭合的．让 $b, c \in [0, \infty]$, 定义

$$\mathrm{Hom}(b, c) = [b, c] = \begin{cases} c - b, & 若\ c > b \\ 0, & 若\ c \leqslant b \end{cases}.$$

立即可见

$$\frac{a + b \geqslant c}{a \geqslant [b, c]}.$$

**定义 6** $(\mathcal{U}, \otimes, I)$ 是一个 monoidal 范畴． $X$ 是一个 $\mathcal{U}$-enriched 范畴．若对 $X$ 中任意两个对象 $A, B$, $X(A, B)$ 是 $\mathcal{U}$ 中的一个对象，并且有

复合映射 $m_{ABC}: \ X(A,B)\otimes X(B,C) \longrightarrow X(A,C)$ (相当于 $(f,g)\longmapsto g\circ f$),

单位映射 $j_A: I \longrightarrow X(A,A)$ (相当于 $1_A: \ A \longrightarrow A$).

在一般范畴中, 映射的复合是可结合的. $(h\circ g)\circ f = h\circ(g\circ f)$; 单位映射满足 $f\circ 1_A = f = 1_B\circ f$. 在 enriched 范畴中这两个性质由以下两个可换图形表示.

$$
\begin{array}{ccc}
(X(A,B)\otimes X(B,C))\otimes X(C,D) & \xrightarrow{a} & X(A,B)\otimes(X(B,C)\otimes X(C,D)) \\
\downarrow m\otimes 1 & & \downarrow 1\otimes m \\
X(A,C)\otimes X(C,D) & & X(A,B)\otimes X(B,D) \\
& {\searrow}^{m} \quad {\swarrow}^{m} & \\
& X(A,D) &
\end{array}
$$

$$
\begin{array}{ccccc}
X(A,B)\otimes X(B,B) & \xrightarrow{m} & X(A,B) & \xleftarrow{m} & X(A,A)\otimes X(A,B) \\
\uparrow 1\otimes j & \nearrow r & & \nwarrow l & \uparrow j\otimes 1 \\
X(A,B)\otimes I & & & & I\otimes X(A,B)
\end{array}
$$

若取 monoidal 范畴为 $\mathcal{S}$, Cat, **2**, Ab(可换群的范畴), DG–R–Mod (graded $R$– 模), 和 $[0,\infty]$, 那么 $\mathcal{U}$-enriched 范畴则分别是我们熟悉的, 通常的范畴, 2– 范畴, poset, 可加范畴 (additive category), 可微分次范畴 (differential graded category), 以及 (广义) 度量空间.

若 $X$ 是一个 **2**-enriched 范畴, 则有 $X(x,y)\in \mathbf{2}$, 并且

$$
\begin{array}{lrl}
m_{xyz}: & X(x,y)\wedge X(y,z) & \leqslant X(x,z) \\
j_x \ : & 1 & \leqslant X(x,x).
\end{array}
$$

我们在 $X$ 上定义一个二元关系 $\leqslant$:

$$x,y\in X, \ x\leqslant y \text{ 若有 } X(x,y)=1.$$

那么由 $m_{xyz}$ 和 $j_x$, 二元关系 $\leqslant$ 满足

1) $x \leqslant y,\ y \leqslant z \Longrightarrow x \leqslant z$,

2) $x \leqslant x$.

这样 $X$ 是一个 poset.

对广义度量空间的情况，我们要在后面给以详细说明.

两个普通范畴之间的函子 $F:\ X \longrightarrow Y$, 将 $X$ 的对象送到 $Y$ 的对象，$X$ 中的映射送到 $Y$ 中的映射，并且满足

$$F(g \circ f) = F(g) \circ F(f),$$
$$F(1_A) = 1_{F(A)}.$$

两个 $\mathcal{U}$- 范畴 $X, Y$ 之间的 $\mathcal{U}$- 函子 $T:\ X \longrightarrow Y$, 同样将 $X$ 中的对象送到 $Y$ 中的对象，对于"映射"有 $T_{AB}:\ X(A,B) \longrightarrow Y(TA,TB)$, $T_{AB}$ 是 $\mathcal{U}$ 中的映射. 普通函子满足的两个等式可以表示为以下两个可换图形

$$\begin{array}{ccc} X(A,B)\otimes X(B,C) & \xrightarrow{m} & X(A,C) \\ \big\downarrow{\scriptstyle T\otimes T} & & \big\downarrow{\scriptstyle T} \\ Y(TA,TB)\otimes Y(TB,TC) & \xrightarrow{m} & Y(TA,TC) \end{array}$$

与

$$\begin{array}{ccc} I & \xrightarrow{j} & X(A,A) \\ & \searrow{\scriptstyle j} & \big\downarrow{\scriptstyle T} \\ & & Y(TA,TA) \end{array}$$

若 $\mathcal{U}$ 是 $\mathcal{S}$, Cat, $\mathbf{2}$, Ab, DG-R-Mod, $[0,\infty]$, 那么 $\mathcal{U}$- 函子则分别是通常的函子，2- 函子，不减函数，可加函子，可微分次函子，以及不增函数 (contracting map).

集合 $X$ 上的一个度量是一个函数 $d:\ X \times X \longrightarrow [0,\infty)$, 具有性质

1) $d(x,y)=0$ 当且仅当 $x=y$,

2) $d(x,y)=d(y,x)$,

3) $d(x,y)+d(y,z)\geqslant d(x,z)$.

但是不少时候有用的度量并不一定具有对称性，例如在山区做功的问题. 运一定量的货物从海拔低的地方到海拔高的地方要做功，但从高的地方到低的地方并不做功 (或做负功), 这里没有对称性. 并且从一地到另一相同海拔高度的地方做功为零. 这样，我们有一般的 (广义) 度量的定义.

**定义 7** 集合 $X$ 上的一个 (广义) 度量是一个函数 $d:\ X\times X\longrightarrow[0,\infty]$, 具有性质

1) $d(x,x)=0$,

2) $d(x,y)+d(y,z)\geqslant d(x,z)$.

注意， $d$ 可以取值 $\infty$, $d(x,y)=\infty$ 意味着无法由 $x$ 到达 $y$.

我们要以通过常用的方法使非对称度量对称化. 例如

$$\overline{d}(x,y)=d(x,y)+d(y,x),$$

或 $$\overline{\overline{d}}(x,y)=\max\{d(x,y),d(y,x)\}.$$

让 $\mathcal{U}=([0,\infty],\geqslant)$, $X$ 是一个 $\mathcal{U}$- 范畴，则有 $X(x,y)\in\mathcal{U}$, 并且

$$\begin{array}{ll} m_{xyz}: & X(x,y)+X(y,z)\geqslant X(x,z) \\ j_x\ \ : & 0\geqslant X(x,x). \end{array}$$

这正是 (广义) 度量定义中的两个条件. 这样，一个 $\mathcal{U}$- 范畴正是一个度量空间.

若 $X,Y$ 是两个度量空间， $X$ 到 $Y$ 的一个 $\mathcal{U}$- 函子 $f$, 是 $X$ 到 $Y$ 的一个映射 $f:\ X\longrightarrow Y$, 并且 $X(x_1,x_2)\geqslant Y(f(x_1),f(x_2))$. 这样， $f$ 正是一个距离不增函数，或称 Lipschitz 函数 (Lipschitz 常数 $\leqslant 1$).

$(\mathcal{U},\otimes,I)$ 是一个闭合的 monoidal 范畴，记 $\mathcal{U}$-enriched 的范畴与它们之间的 $\mathcal{U}$- 函子构成的范畴为 $\mathcal{U}$- 范畴. 下面我们要证明 $\mathcal{U}$-

范畴也具有张量积，并且也是闭合的.

让 $X,Y$ 是两个 $\mathcal{U}$- 范畴，那么 $X$ 和 $Y$ 张量积 $X\otimes Y$ 也是一个 $\mathcal{U}$ 范畴，它的对象是有序对 $x,y)$，这里 $x,y$ 分别是 $X$ 和 $Y$ 中的对象. 若 $(x_1,y_1),(x_2,y_2)$ 是 $X\otimes Y$ 中的两个对象，那么

$$X\otimes Y((x_1,y_1),(x_2,y_2)) = X(x_1,x_2)\otimes Y(y_1,y_2).$$

若 $X,Y$ 是两个度量空间， $X\otimes Y$ 也是一个度量空间， $X\otimes Y((x_1,y_1),(x_2,y_2)) = X(x_1,x_2)+Y(y_1,y_2)$.

因为 $\mathcal{U}$ 是闭合的，这个张量积有一个 right adjoint

$$\frac{X\otimes Y \longrightarrow Z}{X \longrightarrow Z^Y}.$$

$Z^Y$ 是 $\mathcal{U}$- 函子范畴. $Z^Y$ 的对象是从 $Y$ 到 $Z$ 的 $\mathcal{U}$- 函子，对象之间的映射是 $\mathcal{U}$- 函子之间的 $\mathcal{U}$- 自然变换. 若 $f,g: Y\longrightarrow Z$ 是两个 $\mathcal{U}$- 函子， $f$ 到 $g$ 的自然变换对象 $Z^Y(f,g)$ 定义为如下 equalizer.

$$Z^Y(f,g)\longrightarrow \prod_{y\in Y} Z(f(y),g(y)) \overset{\tau_1}{\underset{\tau_2}{\rightrightarrows}} \prod_{y,y'\in Y} \mathrm{Hom}\big(Y(y,y'),Z(f(y),f(y'))\big)$$

这里 Hom 是 $\mathcal{U}$ 内的 Hom(这时用到 $\mathcal{U}$ 是闭合的 !). $\tau_1$ 定义如下：

$$\frac{Z(f(y),g(y)) \xrightarrow{\quad\tau_1\quad} \mathrm{Hom}(Y(y,y'),Z(f(y),g(y'))}{Z(f(y),g(y))\otimes Y(y,y') \xrightarrow{1\otimes g} Z(f(y),g(y))\otimes Z(g(y),g(y')) \xrightarrow{m} Z(f(y),g(y'))}$$

$\tau_2$ 定义如下：

$$\frac{Z(f(y'),g(y')) \xrightarrow{\tau_2} \mathrm{Hom}(Y(y,y'),Z(f(y),g(y')))}{\begin{array}{ccc} Y(y,y')\otimes Z(f(y'),g(y')) & & Z(f(y),g(y')) \\ & {\scriptstyle f\otimes 1}\searrow \quad \nearrow{\scriptstyle m} & \\ & Z(f(y),f(y'))\otimes Z(f(y'),g(y')) & \end{array}}$$

这样，$\mathcal{U}$- 函子范畴 $Z^Y$ 也是一个 $\mathcal{U}$- 范畴.

若 $Y,Z$ 是两个度量空间，$\mathcal{U}$- 函子范畴 $Z^Y$ 的对象是从 $Y$ 到 $Z$ 的距离不减函数，$Z^Y$ 上定义有 supmetric: $f,g\in Z^Y$, 那么 $Z^Y(f,g)=\sup_{y\in Y}Z(f(y),g(y))$, 这是因为 $\mathcal{U}=([0,\infty],\geqslant)$ 是一个 poset. 这样，$Z^Y$ 也是一个度量空间.

同样可以构造反变 $\mathcal{U}$- 函子范畴 $Z^{Y^{op}}$. 特别取 $Z$ 为 $\mathcal{U}$, 我们有反变 $\mathcal{U}$- 函子范畴 $\mathcal{U}^{Y^{op}}$, 以及 Yoneda 嵌入 (embedding)

$$Y\longrightarrow \mathcal{U}^{Y^{op}},$$
$$y\longmapsto Y(_,y)\in \mathcal{U}^{Y^{op}}.$$

**Yoneda 引理** Yoneda 嵌入是满的 (full) 和忠实的 (faithful).

这就是说对任意 $y,y'\in Y$, $Y(y,y')\longrightarrow \mathcal{U}^{Y^{op}}(Y(_,y),Y(_,y'))$ 是一个在 $\mathcal{U}$ 中的同构.

若 $\mathcal{U}=(\mathbf{2},\leqslant)$, 一个 $\mathcal{U}$ 范畴是一个 poset, 一个 $\mathcal{U}$- 函子正是一个保序映射，保序映射等价于一个阶理想 (order ideal), 而 $Y(_,y)$ 代表的是主理想. Yoneda 嵌入正是 poset. 由它的主理想代表的 Dedekind 表示.

若 $\mathcal{U}=\mathcal{S}$, 或 $\mathcal{U}=R$- 模，Yoneda 嵌入一般称为正则表示 (regular representation).

若 $\mathcal{U}=([0,\infty],\geqslant)$, Yoneda 引理是说 Yoneda 嵌入是等距的,

$$Y(y,y')=\sup_{y''\in Y}\mathcal{U}(Y(y'',y),Y(y'',y'))=\sup_{y''\in Y}[Y(y'',y),Y(y'',y')].$$

更一般地，给出一个 $\mathcal{U}$- 函子 $i: X \longrightarrow Y$, 可以考虑限制在 $X$ 上的 $Y$ 的 Yeneda 表示：

$$Y \longrightarrow \mathcal{U}^{Y^{\mathrm{op}}} \longrightarrow \mathcal{U}^{X^{\mathrm{op}}}$$

$$y \longmapsto Y(_, y) \longmapsto Y(i(\ ), y).$$

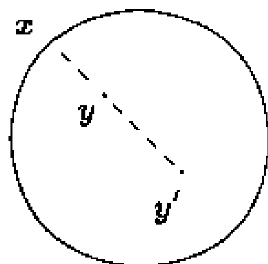
若这个限制也是满的和忠实的，则说 $i$ 是 $\mathcal{U}$-adequate. 如果 $i$ 是一个 inclusion, 则说 $X$ 是 $Y$ 的一个 adequate 子范畴. Adequacy 是一个在表示论里很重要的概念.

如果 $Y$ 是一个度量空间，$Y$ 的子空间 $X$ 是 adequate, 是说对 $Y$ 中的任意两个元素 $y, y'$,

$$\begin{aligned} Y(y, y') &= \sup_{x \in X} \mathcal{U}(Y(i(x), y), Y(i(x), y')) \\ &= \sup_{x \in X} (Y(i(x), y') - Y(i(x), y)). \end{aligned}$$

就是说，对一切 $\varepsilon > 0$, 存在 $x \in X$,

$$Y(i(x), y) + Y(y, y') \leqslant Y(i(x), y') + \varepsilon.$$




例如 $Y$ 是单位圆盘，$X$ 是单位圆，那么 $X$ 是 $Y$ 的一个 adequate 子空间.

3. 凸集的范畴 $\mathcal{C}$ 与度量空间的范畴 $\mathcal{U}$–Cat

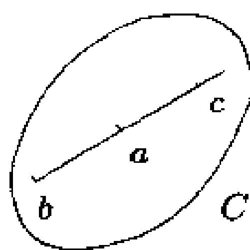
凸集在决策论中有很重要的应用，这是因为决策的集合构成一个凸集，而凸集上定义有一个广义度量 dist, 因之有度量 dist 诱导的拓扑结构. 这样决策的最佳准则可以由度量 dist 来定义，而最佳决策的存在性则有决策空间的拓扑结构的特殊性质 (如紧致性等) 来保证.

由于度量 dist 的存在，这使凸集成为一个度量空间. 这样就有从凸集范畴 $\mathcal{C}$ 到广义度量空间范畴 $\mathcal{U}$–Cat 的一个函子 $\varphi$.

下面我们先定义凸集上的广义度量 dist, 然后讨论函子 $\varphi$.

**定义 8** $C$ 是一个凸集. $a,b\in C$, 定义

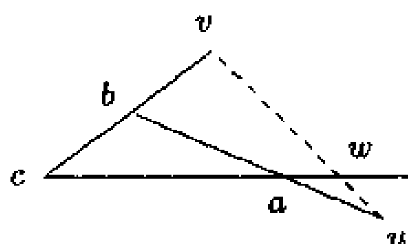
$$\mathrm{dist}(a,b)=-\log\sup_{\substack{\exists c\in C,t\in[0,1]\\ a=tb+(1-t)c}} t.$$




若 $C$ 是欧氏平面 $\mathbf{R}^2$ 的一个子集，那么 $t=\frac{d(a,c)}{d(b,c)}$, 这里 $d(a,c)$ 是 $a$ 到 $c$ 的欧氏距离. 这样 $\mathrm{dist}(a,b)$ 告诉我们以 $b$ 为起点经过 $a$ 的在 $C$ 内的线段的情况.

**命题 6** 如上定义的 dist: $C\times C\longrightarrow[0,\infty]$ 确是一个广义度量.

**证明** 首先易见 $\mathrm{dist}(a,a)=0$. 若




$$a=tb+(1-t)u,$$

$$b=sc+(1-s)v.$$

那么

$$\begin{aligned}a&=t(sc+(1-s)v)+(1-t)u\\&=tsc+t(1-s)v+(1-t)u\\&=tsc+(1-ts)\left(\frac{t(1-s)}{1-ts}v+\frac{1-t}{1-ts}u\right)\end{aligned}$$

因为 $t(1-s)+(1-t)=1-ts, 0\leqslant t(1-s)\leqslant 1-ts, 0\leqslant 1-t\leqslant 1-ts$, 所以 $w=\frac{t(1-s)}{1-ts}v+\frac{1-t}{1-ts}u\in C$. 于是 $ts\leqslant\sup\limits_{\substack{r\in[0,1],w\in C\\ a=rc+(1-r)w}} r.$

$$(-\log\sup t)+(-\log\sup s)\geqslant-\log\sup r.$$

即有 $\mathrm{dist}(a,b)+\mathrm{dist}(b,c)\geqslant\mathrm{dist}(a,c)$.

广义度量 dist 所诱导的拓扑的性质见下一章，随机映射与统计决策论..

**命题 7** $\operatorname{dist}(a,b) = \inf_{\substack{\exists t\in[0,1], c\in C\\ a=tb+(1-t)c}} -\log t.$

**命题 8** $C, B$ 是两个凸集. $f: C \longrightarrow B$ 是一个凸集映射. 那么 $f$ 是一个 dist 距离不减函数:

$$\operatorname{dist}(c_1, c_2) \geqslant \operatorname{dist}(f(c_1), f(c_2)).$$

**证明** 这是因为 $f$ 保持凸运算. 应用命题 7, 由直接计算可得结论.

于是有以下定理.

**定理 6** 存在函子 $\varphi: \mathcal{C} \longrightarrow \mathcal{U}$-Cat.

实际上 $\varphi$ 是一个闭合函子 (closed functor). 因为凸集的范畴 $\mathcal{C}$ 和度量空间的范畴 $\mathcal{U}$-Cat 都是闭合的 monoidal 范畴. 闭合函子是保持闭合结构的函子. 关于闭合函子详细定义，见 [1].

## 参考文献


1 Kelly G M. Basic Concepts of Enriched Category Theory. Cambridge: Cambridge Univ. Press, 1982

2 Lawvere F W. Metric spaces, generalized logic and closed categories. Rend. Sem. Mat. Fis. Milano. 1973, 43: 135~166

3 Meng X. Categories of Convex Sets and of Metric Spaces with Applications to Stochastic Programming and Related Areas. Dissertation, Buffalo: SUNY at Buffalo, 1987

4 Semadeni Z. Banach Spaces of Continuous Functions, Vol.1. Warsaw: PWN-Polish Scientific Publishers, 1971

# 第 15 章

# 随机映射与统计决策论

概率论与统计学以及与它们相关的学科如随机过程，统计决策论的活动范畴基本是两个，一个是可测空间与可测函数的范畴 $\mathfrak{M}$, 另一个是可测空间与随机映射的范畴 $\mathcal{P}(\mathfrak{M})$

$\mathfrak{M}$ 是我们熟悉的范畴. 我们先讨论随机映射的范畴 $\mathcal{P}(\mathfrak{M})$, 以及有关的性质，然后是随机映射的应用.

这一章包括以下几个小节

1. 随机映射的范畴 $\mathcal{P}(\mathfrak{M})$, 以及相关的性质,
2. $\mathcal{P}(\mathfrak{M})(X, Y)$ 上的凸集度量 dist, dist 诱导的拓扑的性质,
3. 概率论中的某些代数结构,
4. 统计决策论,
5. 随机动力程序 (序列决策论，控制的随机过程).

## §1 随机映射的范畴 $\mathcal{P}(\mathfrak{M})$ 以及相关的性质

随机映射 (random map) 又称为概率转移 (probabilistic transition).

**定义 1** $X,Y$ 是两个可测空间，分别具有 $\sigma$- 代数 $\mathcal{A}$ 与 $\mathcal{B}$. 从 $X$ 到 $Y$ 的一个随机映射 $f$ 是一个从 $X\times\mathcal{B}$ 到单位区间 $[0,1]$ 的函数，$f:\ X\times\mathcal{B}\longrightarrow[0,1]$, 具有性质

1) 对任意 $x\in X$, $f(x,_)$ 是 $(Y,\mathcal{B})$ 上的一个概率测度，

2) 对任意可测子集 $B\in\mathcal{B}$, $f(_,B):\ X\longrightarrow[0,1]$ 是一个 $\mathcal{A}$- 可测函数.

记随机映射 $f$ 为 $f:\ X\twoheadrightarrow Y$.

例如在决策论中，$X$ 是信息空间，$Y$ 是观测空间，随机映射 $f:\ X\twoheadrightarrow Y$ 代表从 $X$ 到 $Y$ 的一条充满干扰和噪音的通道，$f(x,B)$ 给出送出信息 $x$, 观测到事件 $B$ 的概率.

又如在马尔科夫链中，$X_n$, $n=0,1,2,\cdots$ 常为有限离散空间. $n$ 级概率转移 $f_n:\ X_n\twoheadrightarrow X_{n+1}$ 即是一个概率转移矩阵.

$X$ 上的一个概率测度 $p$, 可以看为是从只含一个元素的可测空间 1 到 $X$ 的一个随机映射 $p:\ 1\twoheadrightarrow X$.

$X$ 到 $Y$ 的任意一个可测函数 $h:\ X\longrightarrow Y$ 可以看为是一个随机映射 $h(x,B)=\begin{cases}1, & 若\ h(x)\in B,\\ 0, & 若\ h(x)\notin B.\end{cases}$

特别恒等映射 $1_x:\ X\longrightarrow X$, $1_X(x,A)=\begin{cases}1, & x\in A,\\ 0, & x\notin A\end{cases}$ 是一个随机映射.

**定义 2** $f:\ X\twoheadrightarrow Y$, $g:\ Y\twoheadrightarrow Z$ 是两个随机映射. 可测空间 $X,Y,Z$ 分别具有 $\sigma$- 代数 $\mathcal{A},\mathcal{B}$ 和 $\mathcal{C}$, 那么 $f$ 和 $g$ 的复合 $g\circ f:\ X\twoheadrightarrow Z$ 定义如下：$x\in X$, $C\in\mathcal{C}$,

$$g\circ f(x,C)=\int_Y g(y,C)f(x,\mathrm{d}y).$$

若 $X,Y,Z$ 均为有限离散空间，那么随机映射 $f$ 和 $g$ 是概率转移矩阵，而它们的复合 $g\circ f$ 是矩阵的相乘.

根据复合的定义,

$$f\circ 1_X(x,B)=\int_X f(x',B)1_X(x,\mathrm{d}x')=f(x,B),$$

这里 $1_X(x,\mathrm{d}x')=\begin{cases}1, & x=x',\\ 0, & x\neq .x'\end{cases}$

$$\begin{aligned}1_Y\circ f(x,B)&=\int_Y 1_Y(y,B)f(x,\mathrm{d}y)\\&=\int_B f(x,\mathrm{d}y)=f(x,B),\end{aligned}$$

因为 $1_Y(y,B)=1$ 当且仅当 $y\in B$.

所以有 $f\circ 1_X=f$, $1_Y\circ f=f$.

直接由随机映射复合的定义, 可以证明以下命题.

**命题 1** 随机映射的复合是可结合的. 即有 $h\circ(g\circ f)=(h\circ g)\circ f$.

这样, 可测空间与可测空间之间的随机映射构成一个范畴 $\mathcal{P}(\mathfrak{M})$. 而可测空间与可测函数的范畴 $\mathfrak{M}$ 是 $\mathcal{P}(\mathfrak{M})$ 的一个子范畴 $i:\ \mathfrak{M}\hookrightarrow\mathcal{P}(\mathfrak{M})$.

**定义 3** $X$ 是一个可测空间具有 $\sigma$- 代数 $\mathcal{A}$. 让 $\mathcal{P}(X)$ 为 $(X,\mathcal{A})$ 上所有概率测度的集合. 对 $A\in\mathcal{A}, p\in\mathcal{P}(X)$, 定义 $\mathrm{ev}_A(p)=p(A)$, $\mathrm{ev}_A$ 是 $\mathcal{P}(X)$ 到单位区间的一个映射, $\mathrm{ev}_A:\ \mathcal{P}(X)\longrightarrow[0,1]$. 让 $\mathcal{P}(X)$ 具有最小的 $\sigma$- 代数使得每一个 $\mathrm{ev}_A$ 为可测函数. 这样 $\mathcal{P}(X)$ 成为一个可测空间.

**定义 4** $X,Y$ 是两个可测空间, $f:\ X\twoheadrightarrow Y$ 是一个随机映射. 定义

$$\mathcal{P}(f):\ \mathcal{P}(X)\longrightarrow\mathcal{P}(Y),\quad \mathcal{P}(f)(p)=f\circ p.$$

通过直接检验, 可见 $\mathcal{P}(f)$ 是一个可测函数.

这样 $\mathcal{P}$ 成为一个函子, $\mathcal{P}:\ \mathcal{P}(\mathfrak{M})\longrightarrow\mathfrak{M}$.

**定理 1** $\mathfrak{M} \underset{\mathcal{P}}{\overset{i}{\rightleftarrows}} \mathcal{P}(\mathfrak{M})$. $i$ 是 $\mathcal{P}$ 的 left adjoint.

证明见 [8].

我们记 $\mathcal{P}\circ i=\overline{\mathcal{P}}$, 那么 $\overline{\mathcal{P}}$: $\mathfrak{M}\longrightarrow\mathfrak{M}$ 是范畴 $\mathfrak{M}$ 自身到自身的一个函子.

**定义 5** $(X,\mathcal{A})$ 是一个可测空间. 定义

$\eta_X$: $X\longrightarrow\mathcal{P}(X)$, $\eta_X(x)=\delta_x$, $x\in X$, 这里 $\delta_x(A)=\begin{cases}1, & 若\ x\in A,\\ 0, & 若\ x\notin A.\end{cases}$

$\mu_X$: $\overline{\mathcal{P}}\overline{\mathcal{P}}(X)\longrightarrow\overline{\mathcal{P}}(X)$, 对于 $q\in\overline{\mathcal{P}}\overline{\mathcal{P}}(X)$, $A\in\mathcal{A}$, $\mu_X(q)(A)=\int_{p\in\mathcal{P}(X)}\mathrm{ev}_p(A)\,\mathrm{d}q$.

不难检验 $\eta$: $\mathbf{1}_{\mathfrak{M}}\longrightarrow\overline{\mathcal{P}}$, 和 $\mu$: $\overline{\mathcal{P}}\overline{\mathcal{P}}\longrightarrow\overline{\mathcal{P}}$ 是自然变换.

**定理 2** $(\overline{\mathcal{P}},\eta,\mu)$ 构成范畴 $\mathfrak{M}$ 上的一个 monad. 而这个 monad 的 Kleisli 范畴正是随机映射的范畴 $\mathcal{P}(\mathfrak{M})$.

证明见 [8].

可测函数的范畴具有卡氏积.

若 $(X,\mathcal{A})$ 和 $(Y,\mathcal{B})$ 是两个可测空间, 它们的卡氏积即是集合 $X$ 和 $Y$ 的卡氏积, 具有 $\sigma$- 代数 $\mathcal{A}\times\mathcal{B}$, 这里 $\mathcal{A}\times\mathcal{B}$ 是由 $X\times Y$ 上的可测矩形生成的 $\sigma$- 代数 (可测矩形的集合 $\{A\times B\mid A\in\mathcal{A},B\in\mathcal{B}\}$ 并不构成一个 $\sigma$- 代数). $(X\times Y,\mathcal{A}\times\mathcal{B})$ 满足卡氏积唯一性的要求: 若 $(Z,\mathcal{C})$ 是另一可测空间, 有可测函数 $f$: $Z\longrightarrow X$, $g$: $Z\longrightarrow Y$, 那么存在唯一可测函数 $(f,g)$: $Z\longrightarrow X\times Y$, $(f,g)(z)=(f(z),g(z))$, 使得 $\pi_x\circ(f,g)=f$, $\pi_Y\circ(f,g)=g$.

若 $f$: $Z\nrightarrow X$, $g$: $Z\nrightarrow Y$ 是两个随机映射. 对 $X\times Y$ 的任一可测矩形 $A\times B$, $z\in Z$, 定义 $(f,g)(z,A\times B)=f(z,A)\cdot g(z,B)$. 然后应用 Caratheodory 定理, 可将 $(f,g)(z,_)$ 扩展为 $\mathcal{A}\times\mathcal{B}$ 上的一个概率测度. 这样 $(f,g)$: $Z\nrightarrow X\times Y$ 成为一个随机映射, 并且满足 $\pi_x\circ(f,g)=f$, $\pi_Y\circ(f,g)=g$. 但是 $(X\times Y,\mathcal{A}\times\mathcal{B})$ 不是 $(X,\mathcal{A})$ 与 $(Y,\mathcal{B})$ 在范畴 $\mathcal{P}(\mathfrak{M})$ 中的卡氏积. 原因是卡氏积的唯

一性要求不能满足. 下面是一个反例. $X = Y = \{a, b\}$, $X \times Y = \{(a,a),(a,b),(b,a),(b,b)\}$. 投影 $\pi_X : X\times Y \longrightarrow X$, $\pi_Y : X\times Y \longrightarrow Y$ 作为随机映射分别是概率转移矩阵

$$\pi_X = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$
$$\pi_Y = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

让 $Z = 1$, $f = \begin{pmatrix} 0.3 \\ 0.7 \end{pmatrix} : 1 \nrightarrow X$, $g = \begin{pmatrix} 0.5 \\ 0.5 \end{pmatrix} : 1 \nrightarrow Y$.

那么 $(f, g) = \begin{pmatrix} 0.15 \\ 0.15 \\ 0.35 \\ 0.35 \end{pmatrix}$.

$$\pi_X \circ (f,g) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0.15 \\ 0.15 \\ 0.35 \\ 0.35 \end{pmatrix} = \begin{pmatrix} 0.3 \\ 0.7 \end{pmatrix}$$

$$\pi_Y \circ (f,g) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0.15 \\ 0.15 \\ 0.35 \\ 0.35 \end{pmatrix} = \begin{pmatrix} 0.5 \\ 0.5 \end{pmatrix}.$$

但是 $\begin{pmatrix} 0.1 \\ 0.2 \\ 0.4 \\ 0.3 \end{pmatrix} : 1 \nrightarrow X \times Y$ 也满足

$$\pi_X \circ \begin{pmatrix} 0.1 \\ 0.2 \\ 0.4 \\ 0.3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0.1 \\ 0.2 \\ 0.4 \\ 0.3 \end{pmatrix} = \begin{pmatrix} 0.3 \\ 0.7 \end{pmatrix}$$

$$\pi_Y \circ \begin{pmatrix} 0.1 \\ 0.2 \\ 0.4 \\ 0.3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0.1 \\ 0.2 \\ 0.4 \\ 0.3 \end{pmatrix} = \begin{pmatrix} 0.5 \\ 0.5 \end{pmatrix}.$$

**定义 6** $f: X \twoheadrightarrow X', g: Y \twoheadrightarrow Y'$ 是两个随机映射. 定义 $f \times g((x,y), A' \times B') = f(x, A') \cdot g(y, B')$.

同样应用 Caratheodory 定理, 将 $f \times g((x,y), _)$ 扩张为 $\mathcal{A}' \times \mathcal{B}'$ 上的一个概率; 进一步 $f \times g$ 是一个随机映射.

**命题 2** $T$; $\mathcal{P}(\mathfrak{M}) \times \mathcal{P}(\mathfrak{M}) \longrightarrow \mathcal{P}(\mathfrak{M})$,

$T((X, \mathcal{A}), (Y, \mathcal{B})) = (X \times Y, \mathcal{A} \times B)$,

$T((f, g)) = f \times g$,

$T$ 是 $\mathcal{P}(\mathfrak{M})$ 的一个张量.

## §2 $\mathcal{P}(\mathfrak{m})(X, Y)$ 上的凸集度量 dist, dist 诱导的拓扑的性质

$(X, \mathcal{A})$,$(Y, B)$ 是两个可测空间. $\mathcal{P}(\mathfrak{M})(X, Y)$ 是 $X$ 到 $Y$ 的随机映射的集合.

$f, g \in \mathcal{P}(\mathfrak{M})(X, Y)$, $t \in [0, 1]$, 那么 $tf + (1-t)g$ 仍然是 $X$ 到 $Y$ 的一个随机映射: 让 $x \in X$, $B \in \mathcal{B}$

1) $tf(x, _) + (1-t)g(x, _)$ 是 $(Y, B)$ 上的一个概率,

2) $tf(_, B) + (1-t)g(_, B)$ 仍是 $\mathcal{A}$- 可测函数. 所以 $\mathcal{P}(\mathfrak{M})(X, Y)$ 是一个凸集.

这样 $\mathcal{P}(\mathfrak{M})(X, Y)$ 上定义有凸集度量 dist,

$$\operatorname{dist}(f,g) = -\log \sup_{\substack{\exists t\in[0,1],\, h\in\mathcal{P}(\mathfrak{M})(X,Y)\\ f=tg+(1-t)h}} t.$$

**定义 7** $r\in\mathbf{R}$, 并且 $r\geqslant 0$, 定义 $\frac{r}{0}=\begin{cases}1, & 若\ r=0,\\ \infty, & 若\ r>0.\end{cases}$

**命题 3**

$$\sup_{\substack{\exists t\in[0,1],\, h\in\mathcal{P}(\mathfrak{M})(X,Y)\\ f=tg+(1-t)h}} t = \inf_{\substack{x\in X\\ B\in\mathcal{B}}} \frac{f(x,B)}{g(x,B)}$$

所以 $\operatorname{dist}(f,g) = -\log \inf\limits_{\substack{x\in X\\ B\in\mathcal{B}}} \frac{f(x,B)}{g(x,B)}$.

**证明** 首先易见 $\inf\limits_{x\in X,B\in\mathcal{B}} \frac{f(x,B)}{g(x,B)} < 1$. 因此我们可以忽略 $g(x,B)=0$ 的情况. 即有

$$\inf_{\substack{x\in X\\ B\in\mathcal{B}}} \frac{f(x,B)}{g(x,B)} = \inf_{\substack{x\in X\\ B\in\mathcal{B}\\ g(x,B)\neq 0}} \frac{f(x,B)}{g(x,B)}.$$

让 $\inf\limits_{g(x,B)\neq 0} \frac{f(x,B)}{g(x,B)} = s_0$, 那么 $\frac{f(x,B)}{g(x,B)} \geqslant s_0$, 即有 $f(x,B) \geqslant s_0 g(x,B)$, 或 $f(x,B)-s_0 g(x,B)\geqslant 0$. 定义 $h(x,B)=\frac{f(x,B)-s_0 g(x,B)}{1-s_0}$, 不难检验 $h\in\mathcal{P}(\mathfrak{M})(X,Y)$. 这样 $f=s_0 g+(1-s_0)h$.

让 $\sup\limits_{\substack{\exists t\in[0,1],\, l\in\mathcal{P}(\mathfrak{M})(X,Y)\\ f=tg+(1-t)l}} t = t_0$, 那么 $s_0\leqslant t_0$.

另一方面, 若 $f=tg+(1-t)l$, 对于 $x\in X$, $B\in\mathcal{B}$, $f(x,B)=tg(x,B)+(1-t)l(x,B)$. 对于 $g(x,B)\neq 0$, $\frac{f(x,B)}{g(x,B)} = t+(1-t)\frac{l(x,B)}{g(x,B)}$, 这说明 $\frac{f(x,B)}{g(x,B)}\geqslant t$. 所以 $\inf\limits_{g(x,B)\neq 0}\frac{f(x,B)}{g(x,B)}\geqslant t$, 或 $s_0\geqslant t_0$, 即有 $s_0=t_0$.

应用以上这个命题, 我们可以讨论随机映射空间 $\mathcal{P}(\mathfrak{M})(X,Y)$ 上由凸集度量 dist 诱引的拓扑的性质. 但我们先讨论凸集度量 dist 的一般性质.

凸集度量 dist 是一个广义度量. 它与一般度量的区别有两点:

1) 不具有对称性,

2) 一般来讲, $\text{dist}(a,b)=0$ 并不意味着 $a=b$.

但是对随机映射的凸集 $\mathcal{P}(\mathfrak{M})(X,Y)$, $\text{dist}(f,g)=0$ 当且仅当 $f=g$.

由于凸集度量 dist 的非对称性, 所以它诱导的拓扑有两种. 让 $C$ 是一个凸集, $c\in C$, $r\in\mathbf{R}$, $r>0$, 以 $a$ 为中心, $r$ 为半径的开球有两种:

1) 协变开球, $B(a,r)=\{c\in C\mid \text{dist}(a,c)<r\}$,

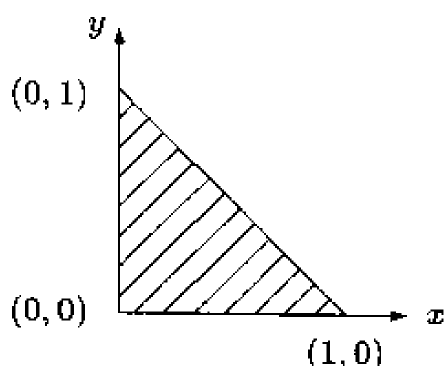
2) 反变开球, $B(r,a)=\{c\in C\mid \text{dist}(c,a)<r\}$. 协变开球与反变开球分别构成 $C$ 上的拓扑基. 这两种拓扑有时性质很不相同.

与一般度量不同的是, 广义度量 dist 是一种有关全局性质的度量. 在欧氏平面 $\mathbf{R}^2$ 上有经典欧氏度量 $d$, $d:\ \mathbf{R}^2\times\mathbf{R}^2\longrightarrow\mathbf{R}$, $d((x_1,y_1),(x_2,y_2))=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$. 若将 $d$ 限制于 $\mathbf{R}^2$ 的一个有限区域 $B$ 上 $d|_B$, 度量 $d|_B$ 与 $d$ 是一致的. 也就是说取 $B$ 中任意两点 $a,b$, 在 $B$ 内用 $d$ 度量 $a,b$ 之间的距离与在 $\mathbf{R}^2$ 上度量所得结果是一致的, 但 dist 却不同.

让 $B$ 为闭单位圆, $a$ 为原点 $(0,0)$, $b=(-1,0)$. 在 $\mathbf{R}^2$ 中, 可以取 $c=(k,0)$, $k>0$, $a=tb+(1-t)c$, 这里 $t=\frac{k}{k+1}$. 这样 $\sup t=1$, $\text{dist}(a,b)=-\log\sup t=0$. 而在 $B$ 中, $t$ 的最大值是 $\frac{1}{2}$, 当 $c=(1,0)$ 时, $t=\frac{1}{2}$, $a=\frac{1}{2}b+\frac{1}{2}c$, $\text{dist}(a,b)=-\log\frac{1}{2}=\log 2$.

下面我们讨论随机映射的凸集 $\mathcal{P}(\mathfrak{M})(X,Y)$.

让 $\mathbf{3}$ 为三个元素的离散空间. $\mathcal{P}(\mathfrak{M})(1,\mathbf{3})$ 是由三个元素生成的自由凸集, $\mathcal{P}(\mathfrak{M})(1,\mathbf{3})$ 可以表示为 $\mathbf{R}^2$ 的一个子集.




首先反变拓扑.

$$a \in \mathcal{P}(1,\mathbf{3}),\ r > 0.$$

$$\begin{aligned} B(r,a) &= \{b \in \mathcal{P}(\mathfrak{M})(1,\mathbf{3}) \mid \mathrm{dist}(b,a) < r\} \\ &= \left\{b \in \mathcal{P}(\mathfrak{M})(1,\mathbf{3}) \mid \min_i \frac{b_i}{a_i} > \mathrm{e}^{-r}\right\}. \end{aligned}$$

若 $a$ 不在边界上，即 $a_i \neq 0$, $i = 1,2,3$, 那么 $b_i > a_i\mathrm{e}^{-r}$.

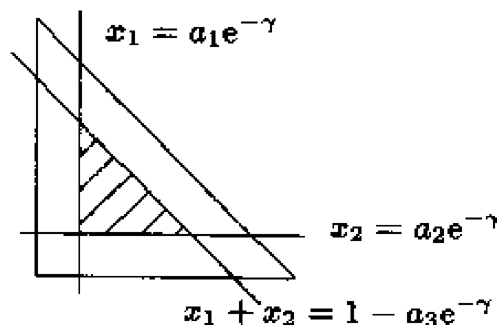
若 $a$ 在边界上，即存在至少一个 $a_i = 0$, 那么 $b_i \geqslant 0 = a_i = a_i\mathrm{e}^{-r}$.

总之有 $b_i \geqslant a_i\mathrm{e}^{-r}$, $i = 1,2,3$. $b_1 \geqslant a_1\mathrm{e}^{-r}$, $b_2 \geqslant a_2\mathrm{e}^{-r}$, $b_3 \geqslant a_3\mathrm{e}^{-r}$, 即 $1-(b_1+b_2) \geqslant a_3\mathrm{e}^{-r}$ 或 $b_1+b_2 \leqslant 1-a_3\mathrm{e}^{-r}$. 所以

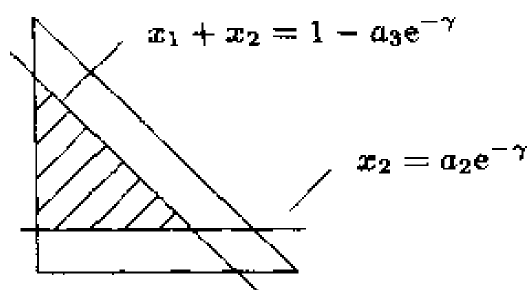
$$\begin{aligned} B(r,a) = \{(x_1,x_2) \in \mathcal{P}(\mathfrak{M})(1,\mathbf{3}) \mid x_1 \geqslant a_1\mathrm{e}^{-r}, \\ x_2 \geqslant a_2\mathrm{e}^{-r},\ x_1+x_2 \leqslant 1-a_3\mathrm{e}^{-r}\}. \end{aligned}$$

等号只在 $a_i = 0$ 时成立.

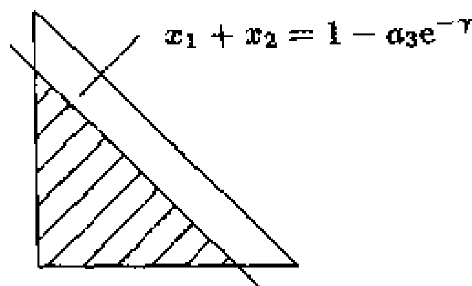
若 $a$ 不在边界上， $B(r,a)$ 是以下区域



若只有一个 $a_i = 0$, 比如 $a_1 = 0$. 那么 $B(r,a)$ 是以下区域




若 $a$ 是三角形的一个顶点, 即有两个 $a_i = 0$, 比如 $a_1 = a_2 = 0$. 那么 $B(r,a)$ 是以下区域




易证以下命题.

**命题 4** $\mathcal{P}(\mathfrak{M})(1,3)$ 上的反变拓扑与 $\mathbf{R}^2$ 上的经典欧几里得拓扑在 $\mathcal{P}(\mathfrak{M})(1,3)$ 上的限制等价.

可以将以上命题推广到 $n$ 维自由凸集 $\mathcal{P}(\mathfrak{M})(1,n+1)$ 上.

第二, 协变拓扑.

$\mathcal{P}(\mathfrak{M})(1,3)$ 上以 $a$ 为中心以 $r$ 为半径的协变开球

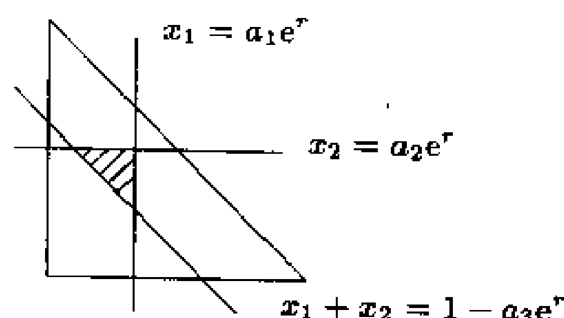
$$\begin{aligned}B(a,r) &= \{b \in \mathcal{P}(\mathfrak{M})(1,3) \mid \operatorname{dist}(a,b) < r\} \\ &= \left\{b \in \mathcal{P}(\mathfrak{M})(1,3) \mid \min_i \frac{a_i}{b_i} > e^{-r}\right\}.\end{aligned}$$

注意, 若 $a_i = 0$, 那么 $b_i = 0$. 这是因为若 $a_i = 0$, $b_i \neq 0$, 则有 $-\log \min_i \frac{a_i}{b_i} = -\log 0 = \infty$.

$\frac{a_i}{b_i} \geqslant \min_i \frac{a_i}{b_i} > \mathrm{e}^{-r}$, 或 $b_i \leqslant a_i \mathrm{e}^{-r}$, 等号只在 $a_i = 0$ 时成立. 这样

$$B(a,r) = \{(x_1, x_2) \in \mathcal{P}(\mathfrak{M})(\mathbf{1},\mathbf{3}) \mid x_1 \leqslant a_1 \mathrm{e}^r, x_2 \leqslant a_2 \mathrm{e}^r,$$
$$x_1 + x_2 \geqslant 1 - a_3 \mathrm{e}^r\}.$$

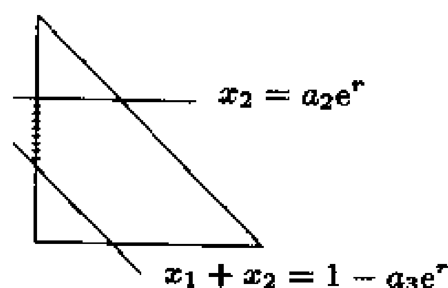
当 $a_i \neq 0$, $i = 1,2,3$ 时 $B(a,r)$ 是以下区域




若只有一个 $a_i = 0$, 比如 $a_1 = 0$, 那么

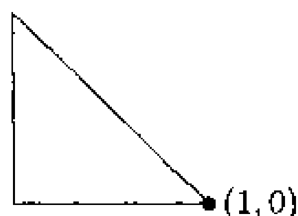
$$B(a,r) = \left\{ \begin{array}{l} x_1 = 0 \\ x_2 < a_2 \mathrm{e}^r \\ x_1 + x_2 > 1 - a_3 \mathrm{e}^r \end{array} \right\}$$

是以下区域




注意 $a_3 = 1 - a_2$, 这样 $1 - a_3 \mathrm{e}^r = 1 - (1 - a_2)\mathrm{e}^r = 1 - \mathrm{e}^r + a_2 \mathrm{e}^r < a_2 \mathrm{e}^r$.

若只有一个 $a_i \neq 0$, 比如 $a_1 \neq 0$, $a_2 = a_3 = 0$, 那么 $B(a,r) = \left\{ \begin{array}{l} x_1 = 1 \\ x_2 = 0 \end{array} \right\}$, $B(a,r)$ 是一个孤立点 $(1,0)$.




所以, $\mathcal{P}(\mathfrak{M})(1,3)$ 上的协变拓扑是它的不同维数开子集 (faces) 上的拓扑的并.

$(X,\mathcal{A})$, $(Y,\mathcal{B})$ 是两个可测空间, $\mathcal{P}(\mathfrak{M})(X,Y)$ 上的反变拓扑有较好的性质.

**定理 3** $\mathcal{P}(\mathfrak{M})(X,Y)$ 上的反变拓扑是 Hausdorff 的, 即是 $T_2$ 的.

**定义 8** $\{f_n\}_{n\in\mathbf{N}} \subseteq \mathcal{P}(\mathfrak{M})(X,Y)$. $\{f_n\}_{n\in\mathbf{N}}$ 是一个 Cauchy 序列, 若对任意 $\varepsilon > 0$, 存在 $N(\varepsilon) \in \mathbf{N}$, 当 $n,m > N$ 时, $\text{dist}(f_n, f_m) < \varepsilon$.

**定理 4** $\mathcal{P}(\mathfrak{M})(X,Y)$ 是 sequential complete, 即是说对任一 Cauchy 序列 $\{f_n\}_{n\in\mathbf{N}}$, 存在 $f \in \mathcal{P}(\mathfrak{M})(X,Y)$, 使得 $\lim\limits_{n\to\infty} \text{dist}(f, f_n) = 0$, 并且 $\lim\limits_{n\to\infty} \text{dist}(f_n, f) = 0$.

**定理 5** $n, m$ 分别是 $n$ 个元素和 $m$ 个元素的离散空间, $\mathcal{P}(\mathfrak{M})(n,m)$ 上的反变拓扑是紧致的.

以上三定理的证明见 [8].

通常我们应用 $\mathcal{P}(\mathfrak{M})(X,Y)$ 上的反变拓扑.

## §3 概率论中的某些代数结构

$f: X \twoheadrightarrow Y$ 是一个随机映射, $p: 1 \twoheadrightarrow X$ 是 $X$ 上的一个概率测度, 那么 $p$ 与 $f$ 的复合 $f \circ p: 1 \twoheadrightarrow Y$ 是 $Y$ 上的一个概

率. 对于 $Y$ 的一个可测集 $B \in \mathcal{B}$, $f \circ p(B) = \int_X f(x, B)\,\mathrm{d}p$.

特别若 $f$ 是一个可测函数 $f:\ X \longrightarrow Y$, 那么 $f \circ p(B) = p(f^{-1}(B))$. $f \circ p$ 称为由 $f$ 诱导的相应于 $p$ 的概率测度. 在概率论中通常取 $Y = \mathbf{R}$ 为实数空间, $\mathbf{R}$ 具有 Borel 子集为 $\sigma$- 代数. $f: X \longrightarrow \mathbf{R}$ 是一个可测函数, 又称为随机变量 (random variable). 这样, $f \circ p:\ 1 \twoheadrightarrow \mathbf{R}$ 是实数空间上的一个由 $f$ 诱导的概率测度, 称为 $f$ 的分布函数 (distribution function)

$$F(u) = f \circ p((-\infty, u)).$$

而 $F$ 的特征函数

$$E(\mathrm{e}^{itf}) = \int_{-\infty}^{\infty} \mathrm{e}^{-itu} \mathrm{d}f \circ p(u) = \int_{-\infty}^{\infty} \mathrm{e}^{-itu} \mathrm{d}F(u).$$

若 $f: X \longrightarrow \mathbf{R}$, $g:\ X \longrightarrow R$ 是两个随机变量. $f$ 与 $g$ 的联合分布 $(f,g) \circ p:\ 1 \overset{p}{\twoheadrightarrow} X \overset{(f,g)}{\longrightarrow} \mathbf{R} \times \mathbf{R}$. $A \times B$ 是一个可测矩形.

$$\begin{aligned}(f,g) \circ p(A \times B) &= \int_X (f,g)(x, A \times B)\,\mathrm{d}p = \int_X f(x, A) \cdot g(x, B)\,\mathrm{d}p \\ &= \int_{f^{-1}(A) \cap g^{-1}(B)} \mathrm{d}p = p(f^{-1}(A) \cap g^{-1}(B)).\end{aligned}$$

特别若 $A = (-\infty, u)$, $B = (-\infty, v)$, 那么

$$\begin{aligned}&(f,g) \circ p((-\infty, u) \times (-\infty, v)) \\ &= p\big(f^{-1}(-\infty, u) \cap g^{-1}(-\infty, v)\big) \\ &= p\{x \in X \mid f(x) < u, g(x) < v\}.\end{aligned}$$

$(f,g) \circ p$ 是乘积空间 $Y \times Y$ 上的一个概率. 还有另一种方法从 $f$ 和 $g$ 构造 $Y \times Y$ 上的一个概率:

$$(f \circ p, g \circ p) : 1 \twoheadrightarrow Y \times Y,$$

$$\begin{aligned}(f \circ p, g \circ p)(A \times B) &= f \circ p(A) \cdot g \circ p(B) \\ &= p(f^{-1}(A)) \cdot p(g^{-1}(B)).\end{aligned}$$

但是一般来说，$p(f^{-1}(A)\cap g^{-1}(B))\neq p(f^{-1}(A))\cdot p(g^{-1}(B))$，除非 $f,g$ 是相互独立的.

这样我们有以下定义

**定义 9** $f,g:X\longrightarrow \mathbf{R}$ 是两个随机变量. $f,g$ 是相互独立的，当且仅当 $(f,g)\circ p=(f\circ p,g\circ p)$.

以上定义的随机变量的独立性与经典定义的独立性是一致的. 这样我们可以将独立性的定义扩展至随机映射：

两个随机映射 $f,g:X\twoheadrightarrow Y$ 是相互独立的，当且仅当乘积空间 $Y\times Y$ 上的两种构造相同，即 $(f,g)\circ p=(f\circ p,g\circ p)$.

$q:1\twoheadrightarrow X\times Y$ 是乘积空间 $X\times Y$ 上的一个概率，$q$ 与射影 $\pi_X,\pi_Y$ 的复合分别给出 $X$ 和 $Y$ 上的概率

$$\pi_X\circ q:1\twoheadrightarrow X,\quad \pi_Y\circ q:1\twoheadrightarrow Y.$$

但是如果只知道 $q$ 在 $X$ 和 $Y$ 上的分量 $\pi_X\circ q,\pi_Y\circ q$ 却无法由此构造 $q$, 因为 $\pi_X\circ q$, $\pi_Y\circ q$ 只给出 $q$ 在 $X$ 和 $Y$ 上的分别作用. 为了重新构造 $q$, 我们需要知道某种混合的作用，这就是所谓的条件概率.

**定义 10** $p$ 是 $X$ 上的一个概率. $f_1:X\twoheadrightarrow Y,f_2:X\twoheadrightarrow Z$ 是两个随机映射 (经典定义中 $f_1,f_2$ 均为可测函数), $(f_1,f_2)\circ p:1\twoheadrightarrow Y\times Z$ 是乘积空间 $Y\times Z$ 上的一个概率. 一个条件概率是一个随机映射 $g_1:Y\twoheadrightarrow Z$, 或是 $g_2:Z\twoheadrightarrow Y$(在经典定义中记 $g_1=p(f_2|f_1)$, $g_2=p(f_1|f_2)$), 使得

$$(f_1,f_2)\circ p=(1_Y,g_1)\circ f_1\circ p,\quad \text{或}\quad (f_1,f_2)\circ p=(g_2,1_Z)\circ f_2\circ p;$$

即以下两个三角形可换

$$
\begin{array}{ccc}
1 & \xrightarrow{f_1\circ p} & Y \\
 & \searrow_{(f_1,f_2)\circ p} & \downarrow{\scriptstyle (1_Y,g_1)} \\
 & & Y\times Z
\end{array}
\qquad
\begin{array}{ccc}
1 & \xrightarrow{f_2\circ p} & Z \\
 & \searrow_{(f_1,f_2)\circ p} & \downarrow{\scriptstyle (g_2,1_Z)} \\
 & & Y\times Z
\end{array}
$$

在上面的定义中，让 $f_1 = f:\ X \nrightarrow Y$ 是一个可测函数，$Z = X$, $f_2 = 1_X:\ X \longrightarrow X$. 这样 $(f,1_X)\circ p:\ 1 \nrightarrow X \nrightarrow Y\times X$ 是 $Y\times X$ 上的一个概率. 这时条件概率 $g:\ Y \nrightarrow X$ 是一个随机映射.

$$
\begin{array}{ccc}
1 & \xrightarrow{f\circ p} & Y \\
 & \searrow_{(f,1_x)\circ p} & \downarrow{\scriptstyle (1_y,g)} \\
 & & Y\times X
\end{array}
$$

$(1_Y,g)\circ f\circ p = (f,1_X)\circ p$. 若 $B\times A$ 是 $Y\times X$ 上的一个可测矩形，则有

$$
\begin{aligned}
(f,1_X)\circ p(B\times A) &= \int_X f(x,B)\cdot 1_X(x,A)\,\mathrm{d}p \\
&= p(f^{-1}(B)\cap A) \\
(1_Y,g)\circ f\circ p(B\times A) &= \int_Y 1_Y(y,B)\cdot g(y,A)\,\mathrm{d}f\circ p \\
&= \int_B g(y,A)\,\mathrm{d}f\circ p
\end{aligned}
$$

所以 $p(f^{-1}(B)\cap A) = \int_B g(y,A)\,\mathrm{d}f\circ p$.

在条件概率的经典定义中，$f:\ X \longrightarrow Y$ 是一个可测函数. 对 $X$ 中的任一可测子集 $A$, 条件概率 $p(y|A) = p(A|f=y)$ 是 $Y$ 上的一个可测函数，并且有 $p(A\cap f^{-1}(B)) = \int_B p(y|A)\mathrm{d}f\circ p$.

比较经典条件概率定义中的 $p(y|A)$, 与我们以上定义 10 中的条件概率 $g: Y \twoheadrightarrow X$, 唯一不同的地方是对于每一个 $y \in Y$, $g(y,_)$ 是 $X$ 上的一个概率测度, 但一般来说, $p(y|_)$ 却不一定是 $X$ 上的一个概率测度. 但若 $X$ 是一个完全可分的度量空间 (complete separable metric space, 如 $X = \mathbf{R}$), 那么 $p(y|_)$ 是 $X$ 上的一个概率 (见 [1]).

## § 4 统计决策论

随机映射在统计决策论中有很重要的应用.

统计决策论的一般模型如下.

$X$ 是信息空间, 具有 $\sigma-$ 代数 $\mathcal{A}$,

$\Omega$ 是观测空间, 具有 $\sigma-$ 代数 $\mathcal{C}$,

$Y$ 是决策空间, 具有 $\sigma-$ 代数 $\mathcal{B}$.

随机映射 $f: X \twoheadrightarrow \Omega$ 代表一条充满干扰和噪音的信息传播渠道. 对 $x \in X, c \in \mathcal{C}$, $f(x,C)$ 代表送出信息 $x$, 观测到事件 $c$ 的概率. 由观测结果我们要确定应采取的行动, 即选取相应的决策. 这一过程也由一个随机映射来描述 $\delta: \Omega \twoheadrightarrow Y$, $\delta$ 称为决策选择. 在一般统计决策论的教科书上, 决策选择 $\delta$ 是一个可测函数. 虽然不少作者意识到决策选择可以是随机的, 概率性质的.

信息空间 $X$ 和决策空间 $Y$ 的关系有以下几种:

1) 损失函数或所得函数

损失函数 (loss function 或 cost function) $l$ 是一个从乘积空间 $X \times Y$ 到实数实间 $\mathbf{R}$ 的可测函数 $l: X \times Y \longrightarrow \mathbf{R}$. 对信息 $x \in X$, 决策 $y \in Y$, $l(x,y)$ 告诉我们, 送出信息 $x$ 而我们选择决策 $y$ 的损失. 类似的所得函数 (reward function) $r: X \times Y \longrightarrow \mathbf{R}$, $r(x,y)$ 告诉我们送出信息 $x$, 我们选择决策 $y$ 的所得.

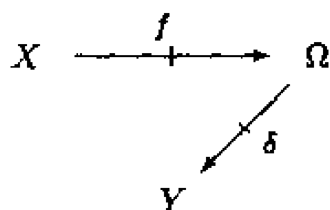
2) 直接联系

客观上说，信息空间和决策空间之间存在着直接的联系，比如说在分类问题上 (医学，机械修理，考古学等等. 见 [7])，这样的直接联系是一个从 $X$ 到 $Y$ 的一一映射；又如在参数估计中，信息空间 $X$，决策空间 $Y$ 均为实数空间 $\mathbf{R}$, $X = Y = \mathbf{R}$，这样直接联系即是 $1_{\mathbf{R}}: \mathbf{R} \longrightarrow \mathbf{R}$. 一般来说，由于干扰和噪音的存在，我们可以用一个随机映射 $g: X \nrightarrow Y$ 来描述这一信息空间与决策空间的联系. 我们称 $g$ 为正确行动.

有不同的方法来确定最佳决策选择.

1) 极小极大准则或极大极小准则

若信息空间 $X$ 上不具有一个先验的概率，我们使用这一准则.




对于任意 $x \in X$, $\delta \circ f(x, _)$ 给出决策空间 $Y$ 上的一个概率. 对于损失函数 $l: X \times Y \longrightarrow \mathbf{R}$,

$$l_\delta(x) = \int_Y l(x, y)\delta \circ f(x, \mathrm{d}y)$$

给出送出信息 $x$，由决策选择 $\delta$ 带来的平均损失.

对于所得函数 $r: X \times Y \longrightarrow \mathbf{R}$,

$$r_\delta(x) = \int_Y r(x, y)\delta \circ f(x, \mathrm{d}y)$$

给出送出信息 $x$，决策选择 $\delta$ 带来的平均所得.

这样，$\sup\limits_{x \in X} l_\delta(x)$ 给出在最不利情况下的损失，$\inf\limits_{x \in X} r_\delta(x)$ 给出在最不利情况下的所得. 我们当然希望在最不利的情况下平均损失越小越好，而平均所得越多越好. 于是有以下定义.

**定义 11**

a. 极小极大准则 (对于损失函数)

$\delta^*: \Omega \rightarrow\!\!\!\!+ Y$ 是一个最佳决策选择，若以下等式成立：$\sup\limits_{x\in X} l_{\delta^*}(x) = \inf\limits_{\delta} \sup\limits_{x\in X} l_\delta(x)$.

b. 极大极小准则 (对于所得函数)

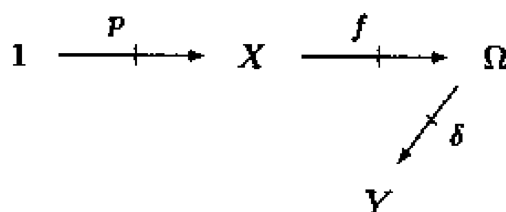
$\delta^*: \Omega \rightarrow\!\!\!\!+ Y$ 是一个最佳决策选择，若以下等式成立 $\inf\limits_{x\in X} r_{\delta^*}(x) = \sup\limits_{\delta} \inf\limits_{x\in X} r_\delta(x)$.

**注** 若决策选择是一个可测函数 $\delta: \Omega \longrightarrow Y$, 那么

$$\begin{aligned}
l_\delta(x) &= \int_Y l(x,y)\delta\circ f(x,\mathrm{d}y) \\
&= \int_Y l(x,y)\int_\Omega \delta(w,\mathrm{d}y)f(x,\mathrm{d}w) \\
&= \int_{Y\times\Omega} l(x,y)\delta(w,\mathrm{d}y)f(x,\mathrm{d}w) \\
&= \int_\Omega l(x,\delta(x))f(x,\mathrm{d}w).
\end{aligned}$$

2) Bayesian 准则

这时信息空间 $X$ 上有一个先验概率 $p: 1 \rightarrow\!\!\!\!+ X$,




随机映射的复合 $\delta\circ f\circ p$ 给出决策空间 $Y$ 上的一个概率. 而 $(1_X, \delta\circ f)\circ p: 1 \xrightarrow{p}\!\!\!\!+ X \xrightarrow{(1_X,\delta\circ f)}\!\!\!\!+ X\times Y$ 是乘积空间 $X\times Y$ 上的一个概率.

对于损失函数 $l: X\times Y\longrightarrow \mathbf{R}$,

$$\begin{aligned} l_\delta &= \int_{X\times Y} l(x,y)((1_X,\delta\circ f)\circ p)(\mathrm{d}x,\mathrm{d}y) \\ &= \int_{X\times Y} l(x,y)\delta\circ f(x,\mathrm{d}y)\,\mathrm{d}p \\ &= \int_X\left(\int_Y l(x,y)\delta\circ f(x,\mathrm{d}y)\right)\mathrm{d}p = \int_X l_\delta(x)\,\mathrm{d}p. \end{aligned}$$

这样 $l_\delta$ 给出决策选择 $\delta$ 带来的平均损失. 同样对所得函数 $r: X\times Y\longrightarrow \mathbf{R}$, 有决策选择 $\delta$ 带来的平均所得 $r_\delta = \int_X r_\delta(x)\,\mathrm{d}p$

我们当然希望平均损失越小越好, 而平均所得越大越好.

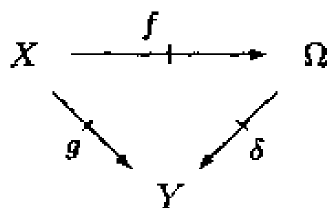
**定义 12** 对损失函数 $l: X\times Y\longrightarrow \mathbf{R}$, $\delta^*: \Omega \to\!\!\!\!\!+ Y$ 是最佳决策选择, 若 $l_{\delta^*} = \inf\limits_\delta l_\delta$;

对所得函数 $r: X\times Y\longrightarrow \mathbf{R}$, $\delta^*: \Omega\to\!\!\!\!\!+ Y$ 是最佳决策选择, 若 $r_{\delta^*} = \sup\limits_\delta r_\delta$.

3) 凸集度量准则

两个可测空间之间的随机映射的集合构成一个凸集, 因而有凸集度量 dist. 特别决策选择的集合 $\mathcal{P}(\mathfrak{M})(\Omega, Y)$ 是一个凸集.

随机映射 $g$ 代表信息空间 $X$ 和决策空间 $Y$ 之间的联系, 称为“正确行动”.




那么我们要求最佳决策选择 $\delta^*$ 使得 $\delta\circ f$ 与 $g$ 离的越“近”越好.

**定义 13** $\delta^*$ 是最佳决策选择, 若 $\mathrm{dist}(\delta^*\circ f, g) = \inf_\delta \mathrm{dist}(\delta\circ f, g)$.

$\mathrm{dist}(_\circ f,g)$ 是一个由决策选择空间 $\mathcal{P}(\mathfrak{M})(\Omega,Y)$ 到 $[0,\infty]$ 的映射，$\mathrm{dist}(_\circ f,g):\mathcal{P}(\mathfrak{M})(\Omega,Y)\longrightarrow[0,\infty]$.

**定义 14** $r,s\in[0,\infty]$, 定义 $[r,s]=\begin{cases}s-r, & 若\ r<s,\\ 0, & 若\ r\geqslant s.\end{cases}$

不难直接检验如上定义的 $[r,s]$ 是 $[0,\infty]$ 上的一个广义度量，即有 $[r,r]=0$, 并且 $[r,s]+[s,t]\geqslant[r,t]$.

**命题 5** $\mathrm{dist}(_\circ f,g):\ \mathcal{P}(\mathfrak{M})(\Omega,Y)\longrightarrow[0,\infty]$ 是一个距离递减函数，即有 $\mathrm{dist}(\delta_1,\delta_2)\geqslant[\mathrm{dist}(\delta_1\circ f,g),\mathrm{dist}(\delta_2\circ f,g)]$, 因而是连续的.

**证明** 这是因为，若 $\delta_1=t\delta_2+(1-t)\delta_3$, 那么 $\delta_1\circ f=t\delta_2\circ f+(1-t)\delta_3\circ f$, 所以 $\mathrm{dist}(\delta_1,\delta_2)\geqslant\mathrm{dist}(\delta_1\circ f,\delta_2\circ f)$; 并且对任意 $r,s,t\in[0,\infty]$, $r+s\geqslant t$ 当且仅当 $r\geqslant[t,s]$.

因为一个紧致空间上的连续函数可以达到它的极大值或极小值，所以由以上命题 5 有以下推论.

**定理 6** 若决策选择空间 $\mathcal{P}(\mathfrak{M})(X,Y)$ 是一个紧致空间，那么最佳决策选择 (定义 13) 存在.

若 $\Omega,Y$ 均为有限空间，那么 $\mathcal{P}(\mathfrak{M})(\Omega,Y)$ 为紧致的. 或者我们可以限制 $\mathrm{dist}(_\circ f,g)$ 在 $\mathcal{P}(\mathfrak{M})(\Omega,Y)$ 的一个紧致子空间上，这样最佳决策选择存在.

下面一个定理给出凸集度量准则与极大极小准则的一个比较.

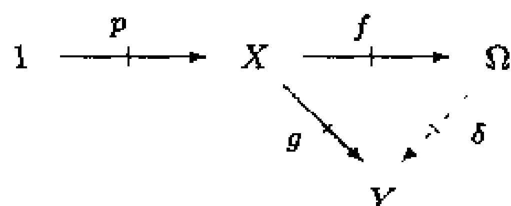
**定理 7** 若信息空间 $X$ 与决策空间 $Y$ 之间的联系正确行动 $g$ 是一个可测函数 $g:\ X\longrightarrow Y$. 我们可以定义一个相应的所得函数 $r:\ X\times Y\longrightarrow\mathbf{R}$,

$$r(x,y)=\begin{cases}1, & 若\ g(x)=y,\\ 0, & 若\ g(x)\neq y.\end{cases}$$

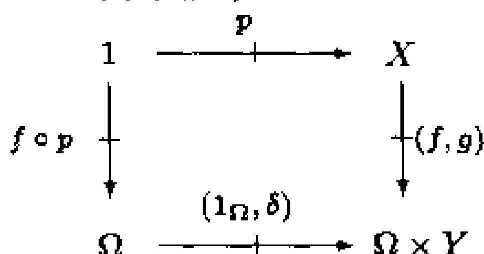
这样由凸集度量准则给出的最佳决策选择与由极大极小准则给出的最佳选择是一致的.

定理的证明见 [8].

在 Bayesian 情况下，信息空间 $X$ 上有一个先验概率 $p: 1 \nrightarrow X$,




这样，$(f,g)\circ p: 1 \nrightarrow \Omega\times Y$ 与 $(1_\Omega,\delta)\circ f\circ p: 1 \nrightarrow \Omega\times Y$, 是乘积空间 $\Omega\times Y$ 上的两个概率




**定义 15** 在 Bayesian 情况下，$\delta^*$ 是一个最佳决策选择，若 $\text{dist}((1_\Omega,\delta^*)\circ f\circ p,(f,g)\circ p)=\inf_\delta \text{dist}\ ((1_\Omega,\delta)\circ f\circ p,(f,g)\circ p)$.

**命题 6** 若存在 $f$ 的条件概率 $\delta_0: \Omega \nrightarrow X$, 满足 $(1_\Omega,\delta_0)\circ f\circ p=(f,1_X)\circ p$, 那么 $\delta^*=g\circ\delta_0$ 是一满足定义 15 的最佳决策选择.

证明

$$\begin{aligned}(1_\Omega,g\circ\delta_0)\circ f\circ p &= 1_\Omega\times g\circ(1_\Omega,\delta_0)\circ f\circ p\\ &= 1_\Omega\times g\circ(f,1_X)\circ p=(1_\Omega\circ f,g\circ 1_X)\circ p=(f,g)\circ p.\end{aligned}$$

这样 $\text{dist}((1_\Omega,g\circ\delta_0)\circ f\circ p,(f,g)\circ p)=0$.

特别，当 $X=Y$, $g=1_X$ (例如参数估计), 那么 $\delta^*=\delta_0$ 是干扰通道 $f$ 的条件概率.

当信息空间与决策空间是相同时， $X=Y$, 而正确行动 $g$ 是 $X$ 的恒等映射时，常用 maximum likelihood 方法构造最佳决策选择.

$f$ 是一条充满噪音的传播渠道 $f: X \nrightarrow \Omega$. 用 maximum likelihood 方法构造的决策选择 $\delta: \Omega \longrightarrow X$ 是一个可测函数. 它的基本思想是将观测空间的元素 $w$ 送到最可能有此结果的信息 $\delta(w) \in X$, 即有 $f(\delta(w), w) = \max_{x \in X} f(x, w)$. 若有多于一个的这样的 $x$, 取其中之一为 $\delta(w)$.

$$f \circ \delta(w, w) = \sum_{x \in X} f(x, w)\delta(w, x) = f(\delta(w), w) = \max_{x \in X} f(x, w).$$

在这种情况下 $(X = Y,\ g = 1_X)$, 凸集度量准测下的最佳决策选择 $\delta^*$ 定义为

$$\text{dist}(f \circ \delta^*, 1_\Omega) = \inf_\delta \text{dist}(\delta \circ f, 1_\Omega).$$

**定理 8** 用 maximum likelihood 方法构造的最佳决策选择 $\delta^*$ 是在凸集度量准则下, 所有可测函数决策选择 $\delta: \Omega \longrightarrow X$ 中的最佳者.

**证明** 我们要证明 $\text{dist}(f \circ \delta^*, 1_\Omega) = \inf_\delta \text{dist}(f \circ \delta, 1_\Omega)$. 这相当于证明

$$-\log \inf_{w, w' \in \Omega} \frac{f \circ \delta^*(w, w')}{1_\Omega(w, w')} \leqslant -\log \inf \frac{f \circ \delta(w, w')}{1_\Omega(w, w')}, \quad \text{对任意 } \delta.$$

但是 $1_\Omega(w, w') = 1$ 当且仅当 $w = w'$, 即相当于

$$\inf_{w \in \Omega} f \circ \delta^*(w, w) \geqslant \inf_{w \in \Omega} f \circ \delta(w, w).$$

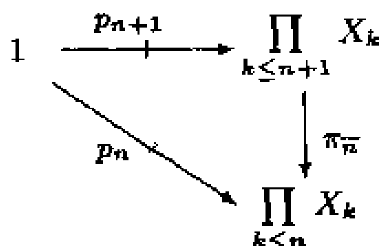
但是

$$\begin{aligned} f \circ \delta^*(w, w) &= \sum_{x \in X} f(x, w)\delta^*(w, x) \\ &= f(\delta^*(w), w) = \max_{x \in X} f(x, w) \\ &\geqslant f(\delta(w), w) = f \circ \delta(w, w). \end{aligned}$$

## § 5 随机动力程序 (序列决策论, 控制的随机过程)

一般教科书上随机过程的定义有三类:

a. 一个随机过程 $\{p_n\}_{n=1,2,\cdots}$ 是一列状态空间乘积上的概率分布 $p_n: 1 \to\!\!\!\!\!+ \prod_{k\leqslant n} X_k$, 这些概率分布是相容的, 即有 $\pi_{\overline{n}} \circ p_{n+1} = p_n$.




b. 一个随机过程 $\{f_n\}_{n=1,2,\cdots}$ 是一列随机变量 (实值可测函数), $f_1,\cdots,f_n$ 的联合分布 $F_n$ 是 $\mathbf{R}^n$ 上的一个概率分布, $n = 1,2,\cdots$. 这列分布 $\{F_n\}$ 当然是相容的.

c. 另一种定义是马尔可夫链的定义.

一个随机过程是一列随机映射 $q_n: X_n \to\!\!\!\!\!+ X_{n+1}, n = 1,2,\cdots$, 加上一个初始概率 $q_0: 1 \to\!\!\!\!\!+ X_1$.

这样我们也可以造一列相容的乘积状态空间 $\prod_{k\leqslant n} X_k$ 上的概率:

$$\overline{q}_1 = q_0: 1 \to\!\!\!\!\!+ X_1,$$

$$\overline{q}_2 = (1_{X_1}, q_1) \circ q_1: 1 \to\!\!\!\!\!+ X_1 \to\!\!\!\!\!+ X_1 \times X_2,$$

$$\vdots$$

$$\overline{q}_n = \left(1_{\prod\limits_{k\leqslant n-1} X_k}, q_{n-1} \circ \pi_{n-1}\right) \circ \overline{q}_{n-1} : 1 \twoheadrightarrow \prod_{k\leqslant n-1} X_k \twoheadrightarrow \prod_{k\leqslant n} X_k,$$

$\vdots$

注意，这三种定义并不等价，这是因为不同的随机变量序列或随机映射序列可以给出乘积空间上的相同的概率.

随机动力程序 (stochastic dynamic programming) 或序列决策论 (sequential decision problem), 又称为控制随机过程 (controlled stochastic process). 它的基本特点是：动力 (dynamics) 或转换 (transformation) 不仅依赖于状态 (states), 而且依赖于决策 (decision).

随机动力程序的模型如下：

$\mathbf{N} = \{0, 1, 2, \cdots\}$.

1) 状态空间 $X_n$, $n \in \mathbf{N}$;

2) 决策空间 $A_n$, $n \in \mathbf{N}$;

3) 动力 (转移)

$$T_n : \prod_{k\leqslant n} X_k \times \prod_{k\leqslant n} A_k \twoheadrightarrow X_{n+1},$$

在马尔可夫情况下，动力不依赖于历史， $T_n : X_n \times A_n \twoheadrightarrow X_{n+1}$;

4) 决策选择 $\delta_0 : X_0 \twoheadrightarrow A_0$,

$$\delta_n : \prod_{k\leqslant n} X_k \times \prod_{k\leqslant n-1} A_k \twoheadrightarrow A_n, \quad n \geqslant 1.$$

**注** a. 在 [2] 中， Bellman 的定义是平稳马尔可夫程序，即 $X_n = X, A_n = A, n \in \mathbf{N}$, 并且 $T_n : X \times A \longrightarrow X, \delta_n : X \times A \longrightarrow A$.

同样情况在 Gihman [5].

b. 若让 $T_n, \delta_n \in \mathfrak{M}$, 为可测函数，那么我们称这样的动力程序为确定的动力程序 (deterministic dynamic programming), 如 [2]; 若 $T_n, \delta_n \in \mathcal{P}(\mathfrak{M})$, 为随机映射，我们则得到随机动力程序.

5) 最佳决策选择的准则 (criteria of optimal policy).

这里我们讨论所得函数准则：

在每一阶段 $n$, 有所得函数 $r_n: X_n \times A_n \longrightarrow \mathbf{R}$.

a. 确定型 (deterministic case)

若选择了一个初始状态 $x_0 \in X$, 以及一列决策 $a_0, a_1, a_2, \cdots$, 则有一列相应的状态 $x_1 = T_0(x_0, a_0)$, $x_2 = T_1(x_0, x_1, a_0, a_1), \cdots$. 定义 $f_N(x_0) = \max \sum\limits_{k=0}^{N} r_k(x_k, a_k)$, $f_N(x_0)$ 给出选择了初始状态 $x_0$ 在阶段 $N$ 的最大所得. $f_N(x_0)$ 是 $T_n, n = 0, 1, 2, \cdots, N-1$ 的函数.

若确定了一列决策选择 $\delta_{n-1}: \prod\limits_{k\leqslant n} X_k \times \prod\limits_{k\leqslant n-1} A_k \twoheadrightarrow A_n, n = 1, 2, \cdots$, 那么有 $x_0, a_0 = \delta_0(x_0)$, $x_1 = T_0(x_0, a_0)$, $a_1 = \delta_1(x_0, x_1, a_0)$, $x_2 = T_1(x_0, x_1, a_0, a_1), \cdots$. $\delta^*$ 是一列最佳决策选择，若与 $\delta^* = \{\delta_0^*, \delta_1^*, \delta_2^*, \cdots\}$ 相应的一列 $x_0, a_0, x_1, a_1, x_2, a_2, \cdots$, 在每一阶段 $N$,

$$\sum_{k=0}^{N} r_k(x_k, a_k) = f_N(x_0).$$

b. 随机型

$$T_n: \prod_{k\leqslant n} X_k \times \prod_{k\leqslant n} A_k \twoheadrightarrow X_{n+1},$$

$$\delta_n: \prod_{k\leqslant n} X_k \times \prod_{k\leqslant n-1} A_k \twoheadrightarrow A_n$$

均为随机映射.

对 $(x_0, \cdots, x_n, a_0, \cdots, a_n) \in \prod\limits_{k\leqslant n} X_k \times \prod\limits_{k\leqslant n} A_k$, 有一个 $X_{n+1}$ 上的概率, $T_n(_ \mid x_0, \cdots, x_n, a_0, \cdots, a_n)$. 对 $(x_0, \cdots, x_n, a_0, \cdots, a_{n-1}) \in$

$\prod\limits_{k\leqslant n} X_k\times \prod\limits_{k\leqslant n-1} A_k$ 有一个 $A_n$ 上的概率 $\delta_n(\cdot\,|\,x_0,\cdots,x_n,a_0,\cdots,a_{n-1})$. 这样，若给出一个初始概率 $\mu_0$ ： $1 \to\!\!\!\!\to X_0$, 我们有乘积空间 $\prod\limits_{k=0}^{\infty} X_k \times \prod\limits_{k=0}^{\infty} A_k = X\times A$ 上的一个概率 $p_{\mu_0,\delta}$ ： $1 \to\!\!\!\!\to X\times A$. 让 $\left(\prod\limits_{k\leqslant n} B_k\times C_k\right)\times\left(\prod\limits_{k=n+1}^{\infty} X_k\times A_k\right) = B_0\times C_0\times\cdots\times B_n\times C_n\times X_{n+1}\times A_{n+1}\times\cdots$ 为 $X\times A$ 上的一个可测长方体. 这里 $B_k, C_k$ 分别是 $X_k$ 和 $A_k$ 的可测子集，那么

$$
\begin{aligned}
&P_{\mu_0,\delta}\left(\left(\prod_{k\leqslant n} B_k\times C_k\right)\times\left(\prod_{k=n+1}^{\infty} X_k\times A_k\right)\right)\\
&=\int_{B_0}\int_{C_0}\cdots\int_{B_n}\int_{C_n}\delta_n(\mathrm{d}a_n|\,x_0,\cdots,x_n,a_0,\cdots,a_{n-1})\\
&\quad\cdot T_{n-1}(\mathrm{d}x_n|\,x_0,\cdots,x_{n-1},a_0,\cdots,a_{n-1})\cdots\\
&\quad\cdot\delta_0(\mathrm{d}a_0|\,x_0)\mu_0(\mathrm{d}x_0).
\end{aligned}
$$

同样，若 $\mu_m$ 是一个概率 $\mu_m$ ： $1 \to\!\!\!\!\to \prod\limits_{k\leqslant m} X_k\times\prod\limits_{k\leqslant m-1} A_k$, 那么 $P_{\mu_m,\delta}$ 是 $X\times A$ 上的一个概率，对 $n>m$,

$$
\begin{aligned}
&P_{\mu_m,\delta}\left(\left(\prod_{k\leqslant n} B_k\times C_k\right)\times\left(\prod_{k=n+1}^{\infty} X_k\times A_k\right)\right)\\
&=\int_{\prod\limits_{k\leqslant m} B_k\times\prod\limits_{k\leqslant m-1} C_k}\int_{C_m}\cdots\int_{B_n}\int_{C_n}\delta_n(\mathrm{d}a_n|\,x_0,\cdots,x_n,a_0,\cdots,a_{n-1})\\
&\quad\cdot T_{n-1}(\mathrm{d}x_n|\,x_0,\cdots,x_{n-1},a_0,\cdots,a_{n-1})\cdots\\
&\quad\cdot\delta_m(\mathrm{d}a_m|\,x_0,\cdots,x_m,a_0,\cdots,a_{m-1})\mathrm{d}\mu_m.
\end{aligned}
$$

让 $r_{(n)}(x,a)=\sum\limits_{k=0}^{n} r_k(x_k,a_k)$, $(x,a)\in X\times A$,

$$
R_n(\mu,\delta)=R_n=\int_{X\times A} r_{(n)}(x,a)\,\mathrm{d}P_{\mu,\delta}.
$$

对于一个初始概率 $\mu$：$1 \nrightarrow X_0$，$\delta^*$ 为最佳决策选择，若对每一个 $n$，$R_n(\mu, \delta^*) = \sup_{\delta} R_n(\mu, \delta)$.

最佳决策选择的存在依赖于 (1) 决策选择空间在某一拓扑结构下是紧致的，(2) 所得函数是上连续的 (upper semi continuous)，因而可以应用定理，紧致空间上的上连续函数可以达到它的上极限.

决策选择空间上的拓扑结构，一是由状态空间与决策空间上的某种结构所诱导，另一种是运用凸集度量诱导的拓扑.

## 参考文献


1 Ash R B. Real Analysis and Probability. New York: Academic Press, 1972

2 Bellman R, Kalaba R. Dynamic Programming and Modern Control Theory. New York: Academic Press, 1965

3 Brown L D, Doshi B T. Existence of optimal policy in stochastic dynamic programming. Probability and Math. Statistics, 1980, 1: 171～184

4 Cencov N N. Statistical Decision Rules and Optimal Inference. Providence: Amer. Math. Soc., 1982

5 Gihman I I, Skorohod A V. Controlled Stochastic Processes. Heidelberg: Springer–Verlag, 1979

6 Lawvere F W. Metric spaces, generalized logic and closed categories. Rend. Sem. Mat. Fis. Milano, 1973, 43: 135～166

7 Melsa J L, Cohn D L. Decision and Estimation Theory. New York: McGraw–Hill Book Co., 1978

8 Meng X. Categories of Convex Sets and of Metric Spaces with Applications to Stochastic Programming and Related Areas. Dissertation, Buffalo: SUNY at Buffalo, 1987

9 Semadeni Z. Banach Spaces of Continuous Functions, Vol.1. Warsaw: PWN-Polish Scientific Publishers, 1971

10 White D J. Dynamic Programming. Edinburgh: Olive & Boyd, 1969

# 第 16 章

# 凸集度量 dist 的一些有趣性质

$C$ 是一个凸集. $a, b \in C$, $\operatorname{dist}(a,b) = -\log \sup\limits_{\substack{\exists t \in [0,1], c \in C \\ a = tb + (1-t)c}} t$. (见[1])

1. dist 是一个相对的度量, $\operatorname{dist}(a,b)$ 的大小依赖于空间 (宇宙).

通常意义的度量是绝对的度量, 两点之间的距离不论是在子空间中度量, 还是在全空间中度量是一致的. 例如欧氏平面与空间中两点之间的距离. 但是凸集度量 dist 却是一个相对的度量. 下面是一个例子.

$C_1 = [0,1]$ 是单位区间, $C_n = [0,n]$, $C_1 \subseteq C_n$

$a, b \in [0,1]$, (数轴: 0, $a$, $b$, 1)

$\operatorname{dist}_{C_1}(b,a) = \log \frac{1-a}{1-b}$, $\operatorname{dist}_{C_n}(b,a) = \log \frac{n-a}{n-b}$. 而 $\lim\limits_{n\to\infty} \log \frac{n-a}{n-b} = 0$.

中心为 $a$, 半径为 $r>0$ 的开球 $B(r,a)=\{x|\ \mathrm{dist}(x,a)<r\}$.

$$\begin{aligned}B_{C_1}(r,a)&=\{x\in[0,1]\mid a\mathrm{e}^{-r}<x<1-(1-a)\mathrm{e}^{-r}\}\\&=(a\mathrm{e}^{-r},1-(1-a)\mathrm{e}^{-r}),\\B_{C_n}(r,a)&=\{x\in[0,n]\mid a\mathrm{e}^{-r}<x<n-(n-a)\mathrm{e}^{-r}\}\\&=(a\mathrm{e}^{-r},n-(n-a)\mathrm{e}^{-r}).\end{aligned}$$

$B_{C_1}(r,a)\subseteq B_{C_n}(r,a)$.

在 $[0,\infty)$ 内, $\mathrm{dist}(b,a)=0$, 而 $B_{[0,\infty)}(r,a)=[0,\infty)$.

但是 $\mathrm{dist}(a,b)=\log\frac{b}{a}$ 却没有变化, 这是因为 $C_1,C_n$ 在左边具有同一边界 0.

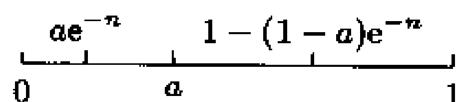
在 $\mathbf{R}=(-\infty,\infty)$ 中, 任意两点 $a,b$ 之间的距离 $\mathrm{dist}(a,b)=0$; 任意开球 $B(r,a)=(-\infty,\infty)$.

当空间增大时两个固定点之间的距离 dist 减小了, 这是因为对比于大的宇宙两点之间的距离相对地变小了. 于是具有固定半径开球的容积增大了. 而当宇宙无限大时, 任意两点间的有限距离相对于无穷大的宇宙成为零, 而任一有限半径的开球扩张为整个宇宙.

这样, 无穷空间中的 dist 不携带任何信息, 这里无穷是指在空间的任一方向上均为无穷.

2. 有限中的无限. 站在空间 (宇宙) 之外观察空间为有限, 但位于空间 (宇宙) 之内发现其为无穷.

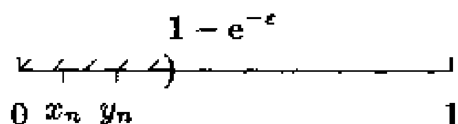
这里我们还是以单位区间 $[0,1]$ 为例. 单位区间 $[0,1]$ 是有限的. 但是对任一正整数 $n$, 我们可以找到 $[0,1]$ 中的两点, 两点之间的 dist 为 $n$. 取 $a\in[0,1]$, 让 $b=a\mathrm{e}^{-n}$ 或 $b=1-(1-a)\mathrm{e}^{-n}$,



则有 $\mathrm{dist}(b,a) = -\log \mathrm{e}^{-n} = n$.

$B(n,a) = (a\mathrm{e}^{-n}, 1-(1-a)\mathrm{e}^{-n})$ 是半径为 $n$, 以 $a$ 为中心的 $[0,1]$ 中的开球. $\bigcup_{n=1}^{\infty} B(n.a) = (0,1) \subset [0,1]$. 若让 $\overline{B}(n,a) = \{x \in [0,1] \mid \mathrm{dist}(x,a) \leqslant n\} = [a\mathrm{e}^{-n}, 1-(1-a)\mathrm{e}^{-n}]$ 为相应的闭球. 同样有 $\bigcup_{n=1}^{\infty} \overline{B}(n.a) = (0,1) \subset [0,1]$.

对于凸集度量 dist, 无法定义类似欧氏空间中的有界空间, 有界子集等. 例如 $B(\varepsilon,0) = [0, 1-\mathrm{e}^{-\varepsilon})$ 是 $[0,1]$ 中以 0 点为中心, $\varepsilon > 0$ 为半径的开球.




让 $x_n = \frac{1}{n}(1-\mathrm{e}^{-\varepsilon})$, $y_n = \frac{n-1}{n}(1-\mathrm{e}^{-\varepsilon})$, $x_n, y_n \in B(\varepsilon, 0)$. 那么 $x_n = ty_n + (1-t)0$, $t = \frac{\frac{1}{n}(1-\mathrm{e}^{-\varepsilon})}{\frac{n-1}{n}(1-\mathrm{e}^{-\varepsilon})} = \frac{1}{n-1}$. 这样 $\mathrm{dist}(x_n, y_n) = \log(n-1) \to \infty$.

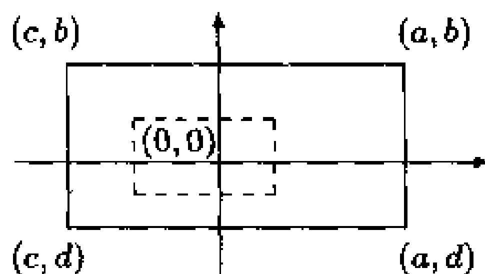
无穷宇宙 $(-\infty, \infty)$ 由无穷多个有限空间 $[n, n+1]$, $n \in \mathbf{Z}$ 构成, 但每一个有限空间 $[n.n+1]$ 本身又是一个无穷的宇宙.

在现代物理学, 天文学中需要这样一个具有相对性质的度量, 这将有助于研究清理多个宇宙, 宇宙大爆炸等理论.

3. 球 $B(r,a)$ 的形状依赖于空间 (宇宙) 的形状.

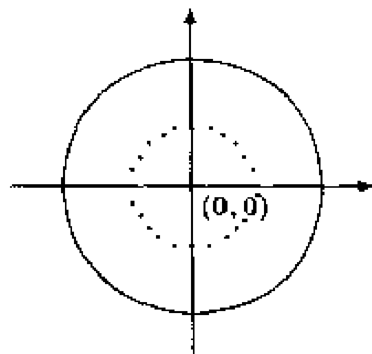
以下是两个例子

空间为长方形 $\left\{(x,y) \in \mathbf{R}^2 \;\middle|\; \begin{matrix} c \leqslant x \leqslant a \\ d \leqslant y \leqslant b \end{matrix}\right\}$, $a, b > 0$, $c, d < 0$.



这样，开球 $B(r,(0,0))=\left\{(x,y)\;\middle|\;\begin{array}{l}c(1-\mathrm{e}^{-r})<x<a(1-\mathrm{e}^{-r})\\ d(1-\mathrm{e}^{-r})<y<b(1-\mathrm{e}^{-r})\end{array}\right\}$ 仍然是一个长方形.

空间为单位圆盘 $D=\{(x,y)\in\mathbf{R}^2\mid x^2+y^2\leqslant 1\}$，那么开球 $B(r,(0,0))=\{(x,y)\mid x^2+y^2<1-\mathrm{e}^r\}$ 仍是一个圆.




4. dist 是一平直度量

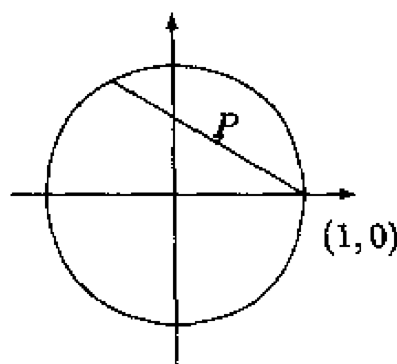
例如欧氏平面 $\mathbf{R}^2$ 中的任一多边形在凸集度量 dist 诱导的拓扑中是紧致的，但是单位圆盘 $D=\{(x,y)\mid x^2+y^2\leqslant 1\}$ 却不是紧致的. 以下是证明.

$0<t<1$, $(x,y)\in D$, 即有 $x^2+y^2\leqslant 1$. 让

$$\begin{aligned}P&=t(1,0)+(1-t)(x,y)\\&=(t+(1-t)x,(1-t)y),\end{aligned}$$

这样

$$\begin{aligned}&(t+(1-t)x)^2+((1-t)y)^2\\&\quad=t^2+2t(1-t)x+(1-t)^2(x^2+y^2)\\&\quad\leqslant t^2+2t(1-t)x+(1-t)^2\\&\quad=1+2t(t-1)(1-x)\\&\quad<1\ ,\end{aligned}$$




所以点 $P$ 不可能是单位圆 $x^2+y^2=1$ 上的点. 这样点 $(1,0)$ 的邻域 $B(r,(1,0))$ 只含有单位圆上的一个点 $(1,0)$. 同样若 $Q$ 是单位圆上的一点， $Q$ 的邻域 $B(r,Q)$ 只含有单位圆上的一点 $Q$. 而若 $Q$ 位于单位圆内，那么 $Q$ 的邻域 $B(r,Q)$ 不含单位圆上的任何一点.

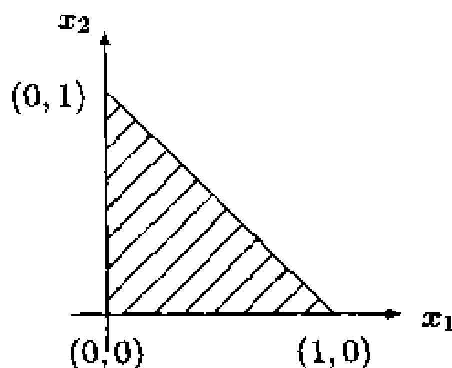
若取开复盖为包含 $D$ 上每一点的一个邻域的集合 $\{B(r,Q)\mid$

$Q \in D\}$, 则不可能找到这个开复盖的一个有限子复盖.

5. 凸集度量 dist 以及熵 (entropy)

让 $C_n$ 为由 $n$ 个元素生成的自由凸集. $C_n$ 是 $n$ 个元素的集合 $X_n = \{x_1, x_2, \cdots, x_n\}$ 上概率的集合, $C_n = \{p = \{p(x_i)\} = \{p_i\} \mid p_i \geqslant 0,\ \sum_{i=1}^{n} p_i = 1\}$.

我们可以将 $C_n$ 看为 $n-1$ 维欧氏空间 $\mathbf{R}^{n-1}$ 的一个子集, 即一个 $n-1$ 维单形 (simplex), $C_n = \{(p_1, p_2, \cdots, p_{n-1}) \in \mathbf{R}^{n-1} \mid p_i \geqslant 0,\ \sum_{i=1}^{n-1} p_i \leqslant 1\}$. 例如 $C_3 = \{(p_1, p_2) \in \mathbf{R}^2 \mid p_1 \geqslant 0, p_2 \geqslant 0, p_1 + p_2 \leqslant 1\}$ 是平面 $\mathbf{R}^2$ 上的一个三角形区域.




$X_n$ 的每一个元素 $x_i$ 代表 $X_n$ 上的一个概率 (deterministic)$\delta_i$,
$$\delta_i(x_j) = \begin{cases} 1, & 若\ i = j, \\ 0, & 若\ i \neq j. \end{cases}$$

对任一概率 $p \in C_n$, $\mathrm{dist}(p, \delta_i) = -\log p_i$, 这是因为若存在 $q \in C_n$, $p = t\delta_i + (1-t)q$, $0 \leqslant t \leqslant 1$. 那么

$$\begin{cases} p_i = t \cdot 1 + (1-t)q_i = t + (1-t)q_i, \\ p_j = t \cdot 0 + (1-t)q_j = (1-t)q_j, \end{cases} \quad j \neq i.$$

为使 $t$ 达到最大值, $q_i$ 应为 0, 我们可以定义 $q$ 如下

1) 若 $p_i = 1$, 让 $q_i = 1, q_j = 0$, 即有 $p = \delta_i = q$,

2) 若 $p_i < 1$, 让 $q_i = 0$, $q_j = \frac{p_j}{1-p_i}$, $j \neq i$.

那么 $t$ 的最大值为 $t = p_i$, $\mathrm{dist}(p, \delta_i) = -\log p_i$. 若 $p_i = \frac{1}{n}$, $\mathrm{dist}(p, \delta_i) = -\log \frac{1}{n} = \log n$.

概率 $p \in C_n$ 的熵定义如下

$$H(p) = -\sum_{i=0}^{n} p_i \log p_i.$$

这里 log 是选择了一个适当底的对数，并且定义 $0\log 0 = 0$. 这正是 Shannon 1948 年在 "A mathematical theory of communication" 中的定义.

易见概率 $p$ 的熵

$$H(p) = -\sum_{i=1}^{n} p_i \log p_i = \sum_{i=1}^{n} p_i \mathrm{dist}(p, \delta_i)$$

. 正是 $p$ 到每一个 $\delta_i$ 的 dist 的加权和 (weighted sum).

6. 单形 $C_n$ 的面结构与 dist 诱导的 preorder

单形 $C_n = \{p \mid p_i \geqslant 0, \sum_{i=1}^{n-1} p_i \leqslant 1\}$ 上由度量 dist 诱导的反变拓扑与协变拓扑有很不相同的性质. $C_n$ 上的反变拓扑等价于 $C_n$ 作为 $\mathbf{R}^{n-1}$ 子集的通常拓扑 (欧氏拓扑). 但 $C_n$ 上的协变拓扑却是它的各维 $(0,1,2,\cdots,n-1)$ 面上协变拓扑的不交并.

在单形 $C_n$ 上定义如下二元关系:

$a, b \in C_n$, $a \leqslant b$ 当且仅当 $\mathrm{dist}(a,b) < \infty$. 易见

1) $a \leqslant a$;

2) 若 $a \leqslant b$, $b \leqslant c$, 则有 $a \leqslant c$.

即 $\leqslant$ 是一个 preorder.

若 $a, b$ 位于单形 $C_n$ 的同一面内, 即 $a_i = 0$ 当且仅当 $b_i = 0$, $i = 1, 2, \cdots, n-1$. 这样 $\mathrm{dist}(a,b) < \infty$, 并且 $\mathrm{dist}(b,a) < \infty$. 那么 $a \leqslant b$, 并且 $b \leqslant a$.

利用这一 preorder, 在单形 $C_n$ 上定义以下等价关系: $a \sim b$ 当且仅当 $a \leqslant b$ 并且 $b \leqslant a$ 即 $\mathrm{dist}(a,b) + \mathrm{dist}(b,a) < \infty$. 易检验这确是一等价关系.

我们有以下结论:

1) $a, b \in C_n$, $a \sim b$ 当且仅当 $a, b$ 位于同一面内.

2) $C_n/\sim$ 是 $C_n$ 的不同面的集合, 即 $C_n$ 包含的不同低维单形的集合.

3) 可以在 $C_n/\sim$ 上定义一个 preorder 关系 $\leqslant'$: $\bar{a}\leqslant'\bar{a}$; $\bar{a}\leqslant'\bar{b}$ (若 $a\neq b$) 当且仅当 $\mathrm{dist}(a,b)=\infty$ 而 $\mathrm{dist}(b,a)<\infty$. 不难检验 $\leqslant'$ 是 well-defined, 并且确实构成一个 preorder.

4) $(C_n/\sim,\leqslant')$ 是单形 $C_n$ 上不同面构成的 poset, $\leqslant'$ 正是通常的面的包含关系.

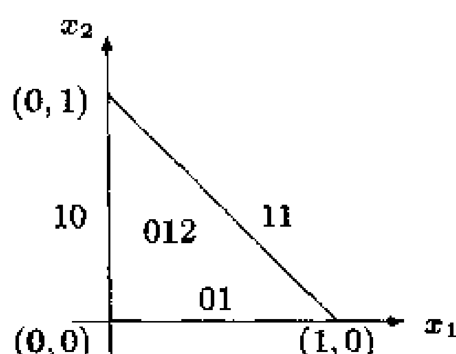
以下以 $C_3$ 为例.

$C_3$ 可以看为平面 $\mathbf{R}^2$ 上的以下三角形区域.

012 代表 $C_3$ 的唯一二维面,

01,10,11 代表 $C_3$ 的三个一维面,

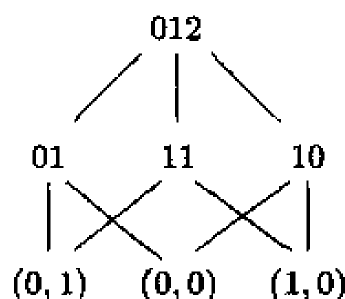
(0,0),(1,0),(0,1) 是 $C_3$ 的三个 0 维面.




因为 0 维面上的点具有两个分量为 0, 1 维面上的点具有一个分量为 0. 若 $a_i\neq 0$, 由 $0=ta_i+(1-t)b_i$ 可得 $t=0$. 即若 $a$ 是 0 维点, $b$ 是一维面上的点或二维面上的点, 则有 $\mathrm{dist}(a,b)=\infty$, 而 $\mathrm{dist}(b,a)<\infty$, 即 $\bar{a}\leqslant'\bar{b}$.

同样若 $a$ 是一维面上的点, $b$ 是二维面上的点, 有 $\mathrm{dist}(a,b)=\infty$, $\mathrm{dist}(b,a)<\infty$. 若 $a$ 是一维面上的点, $b$ 是另一个一维面上的点. 即存在 $i$, $a_i=0$ 而 $b_i\neq 0$; 存在 $j\neq i$, $b_j=0$ 而 $a_j\neq 0$. 这样 $\mathrm{dist}(a,b)=\infty$, 并且 $\mathrm{dist}(b,a)=\infty$.

这样, $(C_3/\sim,\leqslant')$ 的 poset 结构如下:



# 参考文献

1 Meng X. Categories of Convex Sets and of Metric Spaces with Applications to Stochastic Programming and Related Areas. Dissertation, Buffalo: SUNY at Buffalo, 1987

2 Shannon C E. A mathematical theory of communication. Bell System Tech. Jour., 1948, 27: 379~423, 623~656

# 第 17 章

# Monad 和计算语言

范畴论在计算机科学中的应用是多方面的，这一章我们介绍 monad 的概念及其应用.

用 monad 作语义解释的语言系统有两种. 一种用在对多个程序语言做比较时，每一个程序语言对应于一个 monad (为方便起见，我们假设它们是在同一个范畴上的 monad), 研究不同 monad 之间的关系，能得出相应的程序语言之间的关系；另一种是用在一个固定的程序语言中，比较不同程序的相应的性质，两个不同的程序，如何讨论比较它们的性质，如等价性，有效性呢？直观的方法是将程序分别输入计算机，通过执行后的结果加以比较，在很多时候这样做不经济，将程序语言解释在一个有 monad T 的范畴 $\mathcal{C}$ 内，一个类型 B 含有参数为类型 A 的程序对应于一个从值域 A(类型 A) 到计算 TB (类型 B) 的 $\mathcal{C}$ 中的一个映射，这样由范畴内映射的运算，以及 $\mathcal{C}$ 与 T 的性质，可以得到相应的程序的比较性质.

我们先介绍 monad 的概念，然后介绍两类语言系统.

首先是一些符号.

$\mathcal{C}$ 是一个范畴. $f: A \longrightarrow B, g: B \longrightarrow C$ 为 $\mathcal{C}$ 中两个映射，$F$ 与 $g$ 的合成记为 $g \circ f: A \longrightarrow C$. 这是数学上通用的记号.

$1_A: A \longrightarrow A$ 为 $A$ 到 $A$ 的恒等映射,

**注** (1) 有些计算机科学方面的文章将 $f$ 与 $g$ 的合成记为 $f;g$

(2) morphism 一般翻译为 "态射", 我们认为只要注意到上下文的衔接与具体的范畴, 并不会引起概念的混乱, 因而不需要引入那么多的 "生词", 所以我们在这里将 morphism 翻译为映射.

## §1 Monad

**定义 1** 范畴 $\mathcal{C}$ 上的一个 monad $(\mathrm{T},\eta,\mu)$ 由三部分组成, 这里 $T$ 是 $\mathcal{C}$ 到自身的一个函子, $\eta,\mu$ 均为自然变换, $\eta: 1_{\mathcal{C}} \longrightarrow T$, $\mu: T^2 \longrightarrow T$, 并且满足以下可换图形, $A$ 是 $\mathcal{C}$ 中一个对象,

$$\begin{array}{ccc} T^3A & \xrightarrow{\mu_{TA}} & T^2A \\ {\scriptstyle T_{\mu_A}}\downarrow & & \downarrow{\scriptstyle \mu_A} \\ T^2A & \xrightarrow[\mu_A]{} & TA \end{array} \qquad \begin{array}{ccccc} TA & \xrightarrow{\eta_{TA}} & T^2A & \xleftarrow{T_{\eta_A}} & TA \\ & {\scriptstyle 1_{TA}}\searrow & \downarrow{\scriptstyle \mu_A} & \swarrow{\scriptstyle 1_{TA}} & \\ & & TA & & \end{array}$$

$$\mu_A \circ \mu_{TA} = \mu_A \circ T\mu_A \qquad \mu_A \circ \eta_{TA} = 1_{TA} = \mu_A \circ T_{\eta_A}$$

**例 1** $S$ 是集合和映射的范畴, $A$ 是一个集合. 定义 $TA = \mathbf{P}_{\mathrm{fin}}(A) = \{A$ 的有限子集$\}$. $\eta_A: A \longrightarrow TA$, $\eta_A(a) = \{a\}$; $\mu_A: T^2A \longrightarrow TA$. 将 $A$ 的有限个有限子集并起来仍为 $A$ 的一个有限子集. 直接检验可知 $T,\eta,\mu$ 满足 monad 定义的要求.

**例 2** $G$ 是一个固定的群, $X$ 是一个集合, 定义 $TX = G \times X$, 群 $G$ 作用在 $TX$ 上.

$G \times (G \times X) \longrightarrow G \times X$

$(g,(h,x)) \longmapsto (gh,x)$

这正是 $\mu_x$

$\eta_x: X \longrightarrow TX = G \times X$, $\eta_x(x) = (e,x)$ 这里 $e$ 是 $G$ 的单位元.

**例 3**　$X$ 是一个集合，$FX$ 是由 $X$ 生成的自由群. $\eta_x: X \longrightarrow FX$, $\eta_x(x) = x$, $\mu_x$ : $FFX \longrightarrow FX$, 即把自由群 $FX$ 中的有限个元素按顺序摆在一起，看成为 $FX$ 中的一个元素.

**例 4**　$E$ 是一个固定的集合，代表 exception, $TX = X + E$

$\eta_x: X \longrightarrow X + E$,　$\eta_x(x) = \{x\}$,

$\mu_x: X + E + E \longrightarrow X + E$,　$\mu_x(x) = x, \mu_x(e) = e$.

**定义 2**　$(T, \eta, \mu)$ 是 $\mathcal{C}$ 上的一个 monad, $T$ 的一个代数 $(A, h)$ 由两部分组成，其中 $A$ 是 $\mathcal{C}$ 中的一个对象，$h$ 是从 $TA$ 到 $A$ 的在 $\mathcal{C}$ 中的一个映射．满足以下可换图形.

$$\begin{array}{ccc} T^2A & \xrightarrow{Th} & TA \\ {\scriptstyle \mu_A}\downarrow & & \downarrow{\scriptstyle h} \\ TA & \xrightarrow{h} & A \end{array} \qquad \qquad \begin{array}{ccc} A & \xrightarrow{\eta_A} & TA \\ & {\scriptstyle 1_A}\searrow & \downarrow{\scriptstyle h} \\ & & A \end{array}$$

$$h \circ Th = h \circ \mu_A \qquad \qquad h \circ \eta_A = 1_A$$

两个 $T$- 代数 $(A, h)$, $(B, g)$ 之间的同态映射 $f$ : $(A, h) \longrightarrow (B, g)$, 是 $A$ 到 $B$ 的一个映射，并且

$$\begin{array}{ccc} TA & \xrightarrow{h} & A \\ {\scriptstyle Tf}\downarrow & & \downarrow{\scriptstyle f} \\ TB & \xrightarrow{g} & B \end{array}$$

$$g \circ Tf = f \circ h$$

$\mathcal{C}$ 上的 $T$- 代数与 $T$- 代数之间的同态构成一个范畴 $\mathcal{C}^T$. 从 $\mathcal{C}$ 到 $\mathcal{C}^T$ 有一个函子 $F^T$ : $\mathcal{C} \longrightarrow \mathcal{C}^T$, $F^T(A) = (T^2A \xrightarrow{\mu_A} TA) = (TA, \mu_A)$, $F^T(A \xrightarrow{f} B) = (TA \xrightarrow{Tf} TB)$. $F^T$ 有一个 right adjoint $G^T$ : $\mathcal{C}^T \longrightarrow \mathcal{C}$. $G^T(TA \xrightarrow{h} A) = A$, $G^T((A, h) \xrightarrow{f} (B, g)) =$

$(A \xrightarrow{f} B)$.

$G^T$ 正是所谓的 forgetful 函子，忘掉其 $T$- 代数结构.

不少代数结构正是适当 monad 的代数，例如上面的例 2, 例 3.

**定义 3** monad $(T, \eta, \mu)$ 的 Kleisli 范畴 $\mathcal{C}_T$ 定义如下：

$\mathcal{C}_T$ 的对象是 $\mathcal{C}$ 中的对象，$\mathcal{C}_T$ 中从 $A$ 到 $B$ 的一个映射 $f$ 是 $\mathcal{C}$ 中从 $A$ 到 $TB$ 的一个映射，$f: A \longrightarrow TB$, 若 $g: B \longrightarrow TC$, $\mathcal{C}_T$ 中 $f$ 与 $g$ 的合成定义为 $\mu_c \circ Tg \circ f: A \longrightarrow TB \longrightarrow T^2C \longrightarrow C$.

$\mathcal{C}_T$ 中 $A$ 到 $A$ 的恒等映射即是 $\eta_A: A \longrightarrow TA$.

对 Kleisli 范畴 $\mathcal{C}_T$, 有如下函子,

$F_T: \mathcal{C} \longrightarrow \mathcal{C}_T$

$(A \xrightarrow{f} B) \longmapsto (Tf \circ \eta_A: A \xrightarrow{\eta_A} TA \xrightarrow{Tf} TB)$

注意，$Tf \circ \eta_A = \eta_B \circ f$ 这是因为 $\eta$ 是自然变换.

$G_T: \mathcal{C}_T \longrightarrow \mathcal{C}$

$(A \xrightarrow{g} TB) \longmapsto (\mu_B \circ Tg: T_A \xrightarrow{Tg} T^2B \xrightarrow{\mu_B} TB)$

由直接计算可以证明 $F_T$ 是 $G_T$ 的 left adjoint.

若 $(F, G, \eta, \varepsilon)$ 是一对 adjoint 函子，这里 $F: \mathcal{C} \longrightarrow \mathcal{D}, \mathcal{D} \longrightarrow \mathcal{C}$. 让 $T = GF$, $\eta: 1_\mathcal{C} \longrightarrow GF$ 定义 $\mu_A = G\varepsilon_{FA}$, $T^2A = GFGFA \longrightarrow GFA = TA$.

**定理 1** 如上定义的 $(T, \eta, \mu)$ 是 $\mathcal{C}$ 上的一个 monad.

**证明** 我们需要证明 monad 定义中的两个图形可换.

首先，由 $\varepsilon: FG \longrightarrow 1_\mathcal{D}$ 为一个自然变换，于是有下面可换图形

$$\begin{array}{ccc} FGFGFA & \xrightarrow{FG\varepsilon_{FA}} & FGFA \\ {\scriptstyle \varepsilon_{FGFA}}\downarrow & & \downarrow{\scriptstyle \varepsilon_{FA}} \\ FGFA & \xrightarrow{\varepsilon_{FA}} & FA \end{array}$$

$$\varepsilon_{FA} \circ FG\varepsilon_{FA} = \varepsilon_{FA} \circ \varepsilon_{FGFA}$$

对这一等式应用函子 $G$, 我们有 $G\varepsilon_{FA}\circ GFG\varepsilon_{FA}=G\varepsilon_{FA}\circ G\varepsilon_{FGFA}$ 这正是 $\mu_A\circ T\mu_A=\mu_A\circ\mu_{T_A}$ 在以下图形中

$$\begin{array}{ccccc} GFA & \xrightarrow{\eta_{GFA}} & GFGFA & \xleftarrow{GF\eta_A} & GFA \\ & {\scriptstyle 1_{GFA}}\searrow & \downarrow{\scriptstyle G\varepsilon_{FA}} & \swarrow{\scriptstyle 1_{GFA}} & \\ & & GFA & & \end{array}$$

由于 $(F,G,\eta,\varepsilon)$ 是一对 adjoint 函子, 所以有 $G\varepsilon_{FA}\circ\eta_{GFA}=1_{GFA}$, 并且 $G\varepsilon_{FA}\circ GF\eta_A=G(\varepsilon_{FA}\circ F\eta_A)=G(1_{FA})=1_{GFA}$. (见 [1], p80)

**定理 2** adjoint 函子对 $F^T$, $G^T$ 与 $F_T$, $G_T$ 引导的 monad 正是 $(T,\eta,\mu)$.

**定理 3** 在所有引导出 monad $(T,\eta,\mu)$ 的 adjoint 函子对中 $(F^T,G^T,\eta,\varepsilon^T)$ 是最大的一对, 而 $(F_T,G_T,\eta,\varepsilon_T)$ 是最小的一对. 这就是说, 若 $F:\mathcal{C}\longrightarrow\mathcal{D}$, $G:\mathcal{D}\longrightarrow\mathcal{C}$ 是一对引导出 monad $(T,\eta,\mu)$ 的 adjoint 函子, 那么存在唯一函子

$K:\mathcal{D}\longrightarrow\mathcal{C}^T$, 有 $G^TK=G, KF=F^T$;

$L:\mathcal{C}_T\longrightarrow\mathcal{D}$, 有 $GL=G_T, LF_T=F$.

**证明** 首先定义: $K:\mathcal{D}\longrightarrow\mathcal{C}^T$, 若 $f: X\longrightarrow Y$ 为 $\mathcal{D}$ 中映射.

$K(X)=(GFGX\xrightarrow{G\varepsilon_X}GX)$

$$K(f):\quad \begin{array}{ccc} GFGX & \xrightarrow{GFGf} & GFGY \\ {\scriptstyle G\varepsilon_X}\downarrow & & \downarrow{\scriptstyle G\varepsilon_Y} \\ GX & \xrightarrow{Gf} & GY \end{array}$$

因为 $\varepsilon: FG\longrightarrow 1_{\mathcal{D}}$ 为自然变换, 所以 $f\circ\varepsilon_X=\varepsilon_Y\circ GFf$, 因而

$Gf \circ G\varepsilon_X = G\varepsilon_Y \circ GFGf$. 由直接计算可得 $G^T K = G, KF = F^T$.

其次定义 $L: \mathcal{C}_T \longrightarrow \mathcal{D}$, $(A \xrightarrow{g} TB) \longmapsto (\varepsilon_{FB} \circ Fg: FA \xrightarrow{Fg} FTB = FGFB \xrightarrow{\varepsilon_{FB}} FB)$. 那么 $GL(A \xrightarrow{g} TB) = G(\varepsilon_{FB} \circ Fg) = G\varepsilon_{FB} \circ GFg = \mu_B \circ Tg = G_T(g)$; $LF_T(A \xrightarrow{f} B) = L(A \xrightarrow{f} B \xrightarrow{\eta_B} TB) = \varepsilon_{FB} \circ F(\eta_B \circ f) = (\varepsilon_{FB} \circ F\eta_B) \circ Ff = 1_{FB} \circ Ff = Ff$. 所以 $GL = G_T, LF_T = F$.

下面证明函子 $K$ 的唯一性.

因为 $G^T K = G$. 所以 $KA$ 一定具有形式 $KA = (TGA \xrightarrow{h} GA)$. 在 $F^T, G^T$ 的 counit $\varepsilon^T$ 的定义中

$$\mathcal{C}(G^T X, G^T X) \xrightarrow{\sim} \mathcal{C}^T(F^T G^T X, X), \quad 1_{G^T X} \longmapsto \varepsilon^T_X.$$

取 $X = KA$, 于是有 $\varepsilon^T_{KA}: F^T G^T KA \longrightarrow KA$.

但 $KA = (TGA \xrightarrow{h} GA)$ 是 $T$- 代数, 即有以下可换图形

$$F^T G^T KA = \begin{array}{ccc} GFGFGA & \xrightarrow{Th} & GFGA \\ {\scriptstyle \mu_{GA}} \downarrow & & \downarrow {\scriptstyle h} \\ GFGA & \xrightarrow{h} & GA \end{array} = KA$$

所以 $KA = (TGA \xrightarrow{\varepsilon^T_{KA}} GA)$, $h = \varepsilon^T_{KA}$. 但是 $\varepsilon^T_{KA} = K\varepsilon_A$ ([1],p139), 并且 $k\varepsilon_A = G\varepsilon_A$, 即有 $h = G\varepsilon_A$. 这样证明了 $K$ 的唯一性.

同样可证函子 $L$ 的唯一性.

计算机程序语言上要用的是这对最小的 adjoint 函子, 即与 $T$ 的 Kleisli 范畴有关的这对 adjoint 函子 $(F_T, G_T, \eta, \varepsilon_T)$.Kleisli 范畴 $\mathcal{C}_T$ 中的对象 $A$ 是类型 $A$ 的值域 (value), 函子 $T$ 是计算转换, $TA$ 是类型为 $A$ 的计算输出值域, $\mathcal{C}_T$ 中的映射 $f: A \longrightarrow TB$, 对应于计算程序, 输入程序的是类型 $A$ 的值, 而输出的则是类型 $B$ 的计算值.

还有一种等价的方法刻划一个 monad. 这种方法的优点是不涉及范畴论的各种概念，更适于对 monad 概念的直接应用.

**定义 4** 一个 Kleisli triple $(T, \eta, -^*)$ 由以下成份构成： $\mathcal{C}$ 是一个范畴， $\mathrm{Ob}(\mathcal{C})$ 是 $\mathcal{C}$ 中对象的集合； $T$ 是 $\mathrm{Ob}(\mathcal{C})$ 到自身的一个映射 $T\colon \mathrm{Ob}(\mathcal{C}) \longrightarrow \mathrm{Ob}(\mathcal{C})$; 对 $A \in \mathrm{Ob}(\mathcal{C})$, $\eta_A : A \longrightarrow TA$; 若 $f : A \longrightarrow TB$ 为 $\mathcal{C}$ 中一个映射，那么 $f^* : TA \longrightarrow TB$; 它们满足以下要求：

(1) $\eta_A^* = 1_{TA}$,

(2) $f^* \circ \eta_A = f$, 这里 $f : A \longrightarrow TB$,

(3) $g^* \circ f^* = (g^* \circ f)^*$, $g : B \longrightarrow TC$.

**定义 5** 若 $(T, \eta, -^*)$ 是范畴 $\mathcal{C}$ 上的一个 Kleisli triple, 那么它的 Kleisli 范畴 $\mathcal{C}_T$ 定义如下： $\mathcal{C}_T$ 的对象即为 $\mathcal{C}$ 中的对象； $\mathcal{C}_T$ 中 $A$ 到 $B$ 的一个映射是 $\mathcal{C}$ 中 $A$ 到 $TB$ 的一个映射，即有 $\mathcal{C}_T(A, B) = \mathcal{C}(A, TB)$; $\mathcal{C}_T$ 中 $A$ 到 $A$ 的恒等映射是 $\eta_A : A \longrightarrow TA$; $\mathcal{C}_T$ 中映射的合成定义如下， $f : A \longrightarrow TB$, $g : B \longrightarrow TC$, $g^* \circ f : A \xrightarrow{f} TB \xrightarrow{g^*} TC$.

如上定义的 $\mathcal{C}_T$ 确实构成一个范畴. 这里我们要检验

(1) 恒等律 $\eta_B^* \circ f = f, f^* \circ \eta_A = f$;

(2) 结合律 $h^* \circ (g^* \circ f) = (h^* \circ g)^* \circ f$.

$\eta_B^* \circ f = 1_{TB} \circ f$ (Kleisli triple 定义中(1))

$= f$.

$f^* \circ \eta_A = f$ (由 (2)).

$h^* \circ (g^* \circ f) = (h^* \circ g^*) \circ f = (h^* \circ g)^* \circ f$ (由 (3)).

**定理 4** (Manes, 1976). 范畴 $\mathcal{C}$ 上的 Kleisli triple 一一对应于 $\mathcal{C}$ 上的 monad.

**证明** $(T, \eta, -^*)$ 是一个 Kleisli triple, 我们要构造一个相应的 monad $(T, \eta, \mu)$.

若 $f: A \longrightarrow B$, $g: B \longrightarrow C$ 是 $\mathcal{C}$ 中映射，定义 $T(f) = (\eta_B \circ f)^*: TA \longrightarrow TB$. 那么

$$\begin{aligned}
T(g \circ f) &= (\eta_C \circ (g \circ f))^* = ((\eta_C \circ g) \circ f)^* \\
&= (((\eta_C \circ g)^* \circ \eta_B) \circ f)^* \quad \text{(Kleisli triple 定义中(2))} \\
&= ((\eta_C \circ g)^* \circ (\eta_B \circ f))^* \\
&= (\eta_C \circ g)^* \circ (\eta_B \circ f)^* \quad \text{(Kleisli triple 定义中(3))} \\
&= T(g) \circ T(f),
\end{aligned}$$

$$T(1_A) = (\eta_A \circ 1_A)^* = \eta_A^* = 1_{TA}.$$

这样 $T$ 是一个 $\mathcal{C}$ 到自身的函子.

不难检验 $\eta$ 是 $1_{\mathcal{C}}$ 到 $T$ 的一个自然变换.

定义 $\mu_A = 1_{TA}^*: T^2A \longrightarrow TA$. 要检验 $\mu$ 是 $T^2$ 到 $T$ 的一个自然变换，即要检验以下方形可换.

$$\begin{array}{ccc}
T^2A & \xrightarrow{\mu_A} & TA \\
{\scriptstyle T^2f}\downarrow & & \downarrow{\scriptstyle Tf} \\
T^2B & \xrightarrow{\mu_B} & TB
\end{array}$$

$$\begin{aligned}
&\mu_B \circ T^2f = 1_{TB}^* \circ T^2f = 1_{TB}^* \circ (\eta_{TB} \circ (\eta_B \circ f)^*)^* \\
&= ((1_{TB}^* \circ \eta_{TB}) \circ (\eta_B \circ f)^*)^* = (1_{TB} \circ (\eta_B \circ f)^*)^* \\
&= ((\eta_B \circ f)^* \circ 1_{TA})^* = (\eta_B \circ f)^* \circ 1_{TA}^* = Tf \circ 1_{TA}^* = Tf \circ \mu_A
\end{aligned}$$

最后要检验 $(T, \eta, \mu)$ 构成一个 monad.

$$\begin{array}{ccc}
T^3A & \xrightarrow{\mu_{TA}} & T^2A \\
{\scriptstyle T\mu_A}\downarrow & & \downarrow{\scriptstyle \mu_A} \\
T^2A & \xrightarrow{\mu_A} & TA
\end{array}$$

$$\mu_A \circ \mu_{TA} = 1_{TA}^* \circ 1_{T^2A}^* = (1_{TA}^* \circ 1_{T^2A})^*$$
$$= (1_{TA}^*)^* = (1_{TA} \circ 1_{TA}^*)^* = ((1_{TA}^* \circ \eta_{TA}) \circ 1_{TA}^*)^*$$
$$= (1_{TA}^* \circ (\eta_{TA} \circ 1_{TA}^*))^* = 1_{TA}^* \circ (\eta_{TA} \circ 1_{TA}^*) = \mu_A \circ T_{\mu_A}$$

同样

$$\begin{array}{ccccc} TA & \xrightarrow{\eta_{TA}} & T^2A & \xleftarrow{T_{\eta_A}} & TA \\ & {\scriptstyle 1_{TA}} \searrow & \downarrow {\scriptstyle \mu_A} & \swarrow {\scriptstyle 1_{TA}} & \\ & & TA & & \end{array}$$

$$\mu_A \circ \eta_{TA} = 1_{TA}^* \circ \eta_{TA} = 1_{TA},$$
$$\mu_A \circ T_{\eta_A} = 1_{TA}^* \circ (\eta_{TA} \circ \eta_A)^*$$
$$= (1_{TA}^* \circ \eta_{TA} \circ \eta_A)^* \quad = ((1_{TA}^* \circ \eta_{TA}) \circ \eta_A)^*$$
$$= (1_{TA} \circ \eta_A)^* = \eta_A^* = 1_{TA}.$$

这样 $(T, \eta, \mu)$ 是 $\mathcal{C}$ 上一个 monad.

反之，若 $(T, \eta, \mu)$ 是一个 monad，$f: A \longrightarrow TB$ 是 $\mathcal{C}$ 中一个映射，定义 $f^* = \mu_B \circ Tf: TA \longrightarrow T^2B \longrightarrow TB$ 那么不难检验 $(T, \eta, -^*)$ 满足

(1) $\eta_A^* = 1_{TA}$,

(2) $f^* \circ \eta_A = f$,

(3) $g^* \circ f^* = (g^* \circ f)^*$.

这样我们看到 keisli triple 是 monad 的另一种表示方法，以后，我们将根据不同情况使用 Kleisli triple 的定义，或 monad 的定义.

## § 2 简单一般语言

简单一般语言由以下成份组成：

一个类型 (type) 的集合，

一元函数符号 $f: \tau_1 \longrightarrow \tau_2$，

项 $x: \tau_1 \vdash e_1: \tau_2$，

方程 $x: \tau_1 \vdash e_1 =_{\tau_2} e_2$，

一个类型构造符号 (type constructor) $T$，

两个项构造符号 $[-]$, let, 分别满足以下规则：

$$\text{A} \qquad \frac{}{\vdash A\text{type}},$$

$$\text{T} \qquad \frac{\vdash \tau\text{type}}{\vdash T\tau\text{type}},$$

$$\text{var} \qquad \frac{\vdash \ \tau \text{ type}}{x: \tau \vdash x: \tau},$$

$$f: \tau_1 \longrightarrow \tau_2 \qquad \frac{x: \tau \vdash e_1: \tau_1}{x: \tau \vdash f(e_1): \tau_2},$$

$$[-]_T \qquad \frac{x: \tau \vdash e: \tau'}{x: \tau \vdash [e]_T: T\tau'},$$

$$\text{let} \qquad \frac{x: \tau \vdash e_1: T\tau_1 \quad x_1: \tau_1 \vdash e_2: T\tau_2}{x: \tau \vdash (\text{let}_T x_1 \Leftarrow e_1 \text{in} e_2): T\tau_2},$$

$$\text{eq} \qquad \frac{x: \tau_1 \vdash e_1: \tau_2 \quad x: \tau_1 \vdash e_2: \tau_2}{x: \tau_1 \vdash e_1 =_{\tau_2} e_2}.$$

注意，这里项只含有一个自由变量，方程两端含有同样的变量.

简单一般语言之所以称为简单，是因为项只允许含有一个自由变量，且论断只有方程式.

一般语言的语义解释是在一个有多个 monad 的范畴 $C$ 内：

- $\tau$ 是类型， $[\![ \tau ]\!]$ 是 $C$ 中一个对象；

- $x: \tau, 1_{[\![\tau]\!]}: [\![\tau]\!] \longrightarrow [\![\tau]\!]$, $[\![\tau]\!]$ 到自身的恒等映射;
- $f: \tau_1 \longrightarrow \tau_2$, $[\![f]\!]: [\![\tau_1]\!] \longrightarrow [\![\tau_2]\!]$, 是 $\mathcal{C}$ 中一个映射;
- 项 $x: \tau_1 \vdash e_1: \tau_2$ 的语义解释也是 $\mathcal{C}$ 中的一个映射 $[\![\tau_1]\!] \longrightarrow [\![\tau_2]\!]$;
- 类型构造符号 $T$ 解释为 $\mathcal{C}$ 上的一个 monad $(T, \eta, \mu)$, $[\![T\tau]\!] = T[\![\tau]\!]$;
- 若项 $x: \tau \vdash e: \tau'$ 的解释为映射 $g: C \longrightarrow C'$, 那么 $[e]_T: T\tau'$ 的解释为映射 $\eta_{C'} \circ g: C \xrightarrow{g} C' \xrightarrow{\eta_{C'}} TC'$;
- 若 $x: \tau \vdash e_1: T\tau_2$ 的解释为 $g_1: C \longrightarrow TC_1$, $x_1: \tau_1 \vdash e_2: T\tau_2$ 的解释为 $g_2: C_1 \longrightarrow TC_2$, 那么 $x: \tau \vdash (\text{let}_T x_1 \Leftarrow e_1 \text{in} e_2): T\tau_2$ 的解释为映射的合成 $\mu_{C_2} \circ Tg_2 \circ g_1: C \xrightarrow{g_1} TC_1 \xrightarrow{Tg_2} T^2C_2 \xrightarrow{\mu C_2} TC_2$;
- 方程 $x: \tau_1 \vdash e_1 =_{\tau_2} e_2$ 的解释是两个相应映射的相等.

**注** 对任一断言 $x: A \vdash \psi$ 的解释 (在这里是一方程) 或为真或为假.

类型构造符号 $T$ 可以解释为不同的计算函子，它们均为范畴 $\mathcal{C}$ 上的 monad. 常见的有以下几种:

让 $\mathcal{C} = \mathcal{S}$ 为集合的范畴, $A$ 是一个集合.

1. partiality

$TA = A_\perp = A \cup \{\perp\}$, 这里 $\perp$ 代表发散的计算结果.

$\eta_A: A \longrightarrow A_\perp$ 为 inclusion,

$\mu_A: (A_\perp)_\perp \longrightarrow A_\perp$, $\mu_A(a) = a$, $\mu_A(\perp) = \perp$.

2. nondeterminism

$TA = \mathbf{P}_{\text{fin}}(A)$ 是 $A$ 的有限子集的集合, $A$ 的任一有限子集可以看为 $A$ 上的一个概率测度.

$\eta_A: A \longrightarrow \mathbf{P}_{\text{fin}}(A)$, $\eta_A(a) = \{a\}$.

$\mu_A: \mathbf{P}_{\text{fin}}(\mathbf{P}_{\text{fin}}(A)) \longrightarrow \mathbf{P}_{\text{fin}}(A),\ C \longmapsto \cup C.$

3. side-effect

$S$ 为状态 (state) 的集合. 例如 $S$ 可以是输入或输出的序列 $U^*$
$TA = (A \times S)^s$,

$\eta_A: A \longrightarrow (A \times S)^s, \quad a \longmapsto (s \longmapsto (a, s))$, 即 $a \longmapsto (\lambda_s : S. < a, s >)$,

$\mu_A: ((A \times S)^s \times S)^s \longrightarrow (A \times S)^s, \quad (s \longmapsto (f, s')) \longmapsto (s \longmapsto f(s'))$.

4. exceptions

$E$ 是 exception 的集合, $TA = A \dot{\cup} E$, $A \dot{\cup} E$ 为 $A$ 与 $E$ 的不交并,

$\eta_A: A \longrightarrow A \dot{\cup} E$ 为 inclusion,

$\mu_A: A \dot{\cup} E \dot{\cup} E \longrightarrow A \dot{\cup} E,\ \mu_A(a) = a, \mu_A(e) = e.$

5. continuation

$R$ 是计算结果的集合.

$TA = R^{R^A}$,

$\eta_A: A \longrightarrow R^{R^A}, \quad a \longmapsto \hat{a}, \hat{a}(k) = k(a)$, 即 $a \longmapsto (\lambda k : R^A.k(a))$,

若 $f: A \longrightarrow TB = R^{R^B}$, $c \in TA = R^{R^A}$, $f^*: TA \longrightarrow TB$, $f^*(c)(k) = c(a \longmapsto f(a)(k))$, 即 $f^*(c) = (\lambda k : R^B.c(\lambda a : A.f(a)(k)))$. 注意, 第 5 个例子用了 Kleisli triple $(T, \eta, -^*)$ 的定义.

下面给出简单一般语言的推理规则:

1. 自反性 $\dfrac{x : \tau \vdash e : \tau_1}{x : \tau \vdash e =_{\tau_1} e}$

2. 对称性 $\dfrac{x : \tau \vdash e_1 =_{\tau_1} e_2}{x : \tau \vdash e_2 =_{\tau_1} e_1}$

3. 传递性 $\dfrac{x : \tau \vdash e_1 =_{\tau_1} e_2, x : \tau \vdash e_2 =_{\tau_1} e_3}{x : \tau \vdash e_1 =_{\tau_1} e_3}$

4. 同余性 $\dfrac{x:\ \tau \vdash e_1 =_{\tau_1} e_2, f:\ \tau_1 \longrightarrow \tau_2}{x:\ \tau \vdash f(e_1) =_{\tau_2} f(e_2)}$

5. 替换性 $\dfrac{x:\ \tau \vdash e:\ \tau_1, x:\ \tau_1 \vdash \phi}{x:\ \tau \vdash [e/x]\phi}$

6. $[\ ].\xi$ $\dfrac{x:\ \tau \vdash e_1 =_{\tau_1} e_2}{x:\ \tau \vdash [e_1]_T =_{T\tau_1} [e_2]_T}$

7. let.$\xi$ $\dfrac{x:\ \tau \vdash e_1 =_{T\tau_2} e_2, x':\ \tau_1 \vdash e'_1 =_{T\tau_2} e'_2}{x:\ \tau \vdash (\mathrm{let}_T x' \Leftarrow e_1 \mathrm{in}\ e'_1) =_{T\tau_2} (\mathrm{let}_T x' \Leftarrow e_2 \mathrm{in}\ e'_2)}$

8. ass

$$\frac{x:\ \tau \vdash e_1:\ T\tau_1,\ x_1:\ \tau_1 \vdash e_2:\ T\tau_2,\ x_2:\ \tau_2 \vdash e_3 : T\tau_3}{\begin{array}{l} x:\ \tau \vdash (\mathrm{let}_T x_2 \Leftarrow (\mathrm{let}_T x_1 \Leftarrow e_1 \mathrm{in} e_2) \mathrm{in} e_3 \\ =_{T\tau_3} (\mathrm{let}_T x_1 \Leftarrow e_1 \mathrm{in} (\mathrm{let}_T x_2 \Leftarrow e_2 \mathrm{in} e_2)) \end{array}}$$

9. $T.\beta$ $\dfrac{x:\ \tau \vdash e_1:\ \tau_1,\ x_1:\ \tau_1 \vdash e_2:\ T\tau_2}{x:\ \tau \vdash (\mathrm{let}_T x_1 \Leftarrow [e_1]_T \mathrm{in} e_2) =_{T\tau_2} [e_1/x_1]e_2}$

10. $T.\eta$ $\dfrac{x:\ \tau \vdash e_1:\ T\tau_1}{x:\ \tau \vdash (\mathrm{let}_T x_1 \Leftarrow e_1 \mathrm{in} [x_1]_T) =_{T\tau_1} e_1}$

**定义 6** 一个理论 $\mathcal{T}$ 是一组对上述推理规则封闭的方程式.

对理论 $\mathcal{T}$ 可以结合以下范畴 $\mathcal{F}(\mathcal{T})$:

$\mathcal{F}(\mathcal{T})$ 的对象是类型;

两个类型 $\tau_1$ 与 $\tau_2$ 之间的映射是等价类 $[x:\ \tau_1 \vdash e:\ \tau_2]_{\mathcal{T}}$, 这里 $(x:\ \tau_1 \vdash e_1:\ \tau_2) \equiv (x:\ \tau_1 \vdash e_2:\ \tau_2)$ 当且仅当 $(x:\ \tau_1 \vdash e_1 =_{\tau_2} e_2) \in \mathcal{T}$;

$1_\tau = [x:\ \tau \vdash x:\ \tau]_{\mathcal{T}}$;

映射的合成

$$[x:\ \tau_2 \vdash e_2:\ \tau_3]_{\mathcal{T}} \circ [x:\ \tau_1 \vdash e_1:\ \tau_2]_{\mathcal{T}} = [x:\ \tau_1 \vdash [e_1/x]e_2:\ \tau_3]_{\mathcal{T}}.$$

根据理论 $\mathcal{T}$ 的不同性质, 可以要求相应的范畴 $\mathcal{F}(\mathcal{T})$ 具有其它性质.

**定理 5** 简单一般语言的每一个理论 $\mathcal{T}$ 所相应的范畴 $\mathcal{F}(\mathcal{T})$ 具有一个 Kleisli triple $(T, \eta, -^*)$:

$T(\tau) = T\tau$, $\eta_\tau = [x:\ \tau \vdash [x]_T:\ T\tau]_{\mathcal{T}}$,

$$([x:\ \tau_1 \vdash e:\ T\tau_2]_T)^* = [x':\ T\tau_1 \vdash (\text{let}_T x \Leftarrow x'\text{in}e):\ T\tau_2]_T.$$

**证明** 不难直接证明以上定义的 $(T, \eta, -^*)$ 满足 Kleisli trile 定义中的三条要求.

给出一组作为公理的方程式，由这组方程式按推理规则推出的或生成的方程式构成一个理论 $\mathcal{T}$, 按这组推理规则推出的结果对应于在相应范畴中的解释是 sound 和 complete, 即一个方程式可由一组公理经推理规则推出当且仅当在任一满足这组公理的解释中这一方程为真. Soundness 是因为任一解释容纳推理规则; 而 completeness 是因为理论 $\mathcal{T}$ 正是满足在范畴 $\mathcal{F}(\mathcal{T})$ 中规范解释 (canonical interpretation) 的方程式组.

## §3 简单程序语言

应用程序语言可以比较用同一语言写的不同程序的性质，如程序的等价性，有效性等.

在这里只考虑一个 monad. 不同于简单一般语言的是，简单程序语言不是解释在范畴 $\mathcal{C}$ 内，而是解释在这个 monad 的 Kleisli 范畴 $\mathcal{C}_T$ 内

给出范畴 $\mathcal{C}$ 上的一个 monad $(T, \eta, \mu)$. $T$ 的 Kleisli 范畴 $\mathcal{C}_T$ 是唯一决定的. 但若只给出范畴 $\mathcal{C}_T$, 一般来说却无法唯一地再造 $\mathcal{C}$. 为了使这一再造成为可能，我们要求对每一对象 $A$, $\eta_A:\ A \longrightarrow TA$ 为单射 (monomorphism).

由于简单程序语言解释于 Kleisli 范畴 $\mathcal{C}_T$ 中，而 $\mathcal{C}_T$ 中的映射不是 $\mathcal{C}$ 中的映射，所以我们改一元函数符号 $f:\ \tau_1 \longrightarrow \tau_2$ 为一元控制符号 $p:\ \tau_1 \longrightarrow \tau_2$, $p$ 的解释为 $[\![\ \tau_1\ ]\!]$ 到 $T\,[\![\tau_2]\!]$ 的一个映射; 同时我们称项 $x:\ \tau_1 \vdash e:\ \tau_2$ 为一个程序. 它的解释也是由 $[\![\ \tau_1\ ]\!]$ 到 $T\,[\![\tau_2]\!]$ 的一个映射; 并且改相等关系 $=$ 为等价关系 $\equiv$, 等价方程以及存在论断 $ex$ 的解释或为真或为假.

简单程序语言在 $\mathcal{C}_T$ 中的解释：

| | | |
|---|---|---|
| $A$ | $\dfrac{}{\vdash A\text{type}}$ | $[\![A]\!]$ $\mathcal{C}_T$ 中对象 |
| $T$ | $\dfrac{\vdash \tau\text{type}}{\vdash T\tau\text{type}}$ | $C$ $\mathcal{C}_T$ 中对象<br>$TC$ |
| var | $\dfrac{\vdash\ \tau\ \text{type}}{x:\ \tau \vdash x:\ \tau}$ | $C$ $\mathcal{C}_T$ 中对象<br>$\eta_C:\ C \to TC, \mathcal{C}_T$<br>中恒等映射， |
| $p:$<br>$\tau_1 \to \tau_2$ | $\dfrac{x:\ \tau \vdash e_1:\ \tau_1}{x:\ \tau \vdash p(e_1):\ \tau_2}$ | $g:\ C \to TC_1$<br>$\mu_{C_2} \circ TP \circ g:$<br>$C \to TC_1 \to T^2C_2 \to TC_2$ |
| $\mu$ | $\dfrac{x:\ \tau \vdash e:\ T\tau'}{x:\ \tau \vdash \mu(e):\ \tau'}$ | $g:\ C \to T^2C'$<br>$\mu_{C'} \circ g:\ C \to T^2C' \to TC'$ |
| $[_]$ | $\dfrac{x:\ \tau \vdash e:\ \tau'}{x:\ \tau \vdash [e]:\ T\tau'}$ | $g:\ C \to TC'$<br>$\eta_{TC'} \circ g:\ C \xrightarrow{g} TC'$<br>$\xrightarrow{\eta_{TC'}} T^2\tau'$ |
| let | $\dfrac{x:\ \tau \vdash e_1:\ \tau' \quad x_1:\ \tau_1 \vdash e_2:\ \tau_2}{x:\ \tau \vdash (\text{let } x_1 \Leftarrow e_1 \text{in} e_2):\ \tau_2}$ | $g_1:\ C \to TC_1$<br>$g_2:\ C_1 \to TC_2$<br>$\mu_{C_2} \circ Tg_2 \circ g_1:$<br>$C \to TC_1 \to T^2C_2 \to TC_2$ |
| eq | $\dfrac{x:\ \tau_1 \vdash e_1:\ \tau_2 \quad x:\ \tau_1 \vdash e_2:\ \tau_2}{x:\ \tau_1 \vdash e_1 \equiv_{T_2} e_2}$ | $g_1:\ C_1 \to TC_2$<br>$g_2:\ C_1 \to TC_2$<br>$g_1 = g_2$ |
| ex | $\dfrac{x:\ \tau_1 \vdash e:\ \tau_2}{x:\ \tau_1 \vdash e \downarrow \tau_2}$ | $g:\ C_1 \to TC_2$<br>$\exists!\ h:\ C_1 \to C_2$ 使得<br>$c_1 \xrightarrow{g} Tc_2$<br>$g = \eta_{C_2} \circ h,\ \exists! h \searrow \nearrow \eta_{c_2}$<br>$c_2$ |

这里项构造符号 let 起了一个很重要的作用. 从范畴论角度说

let 是 $C_T$ 中映射的合成，从语言运算角度来说 let 代表的是对程序序列连续执行的演算.

下面是简单程序语言的一般推理规则：

1. refl $\dfrac{x:\ \tau \vdash e:\ \tau_1}{x:\ \tau \vdash e \equiv_{\tau_1} e}$

2. symm $\dfrac{x:\ \tau \vdash e_1 \equiv_{\tau_1} e_2}{x:\ \tau \vdash e_2 \equiv_{\tau_1} e_1}$

3. trans $\dfrac{x:\ \tau \vdash e_1 \equiv_{\tau_1} e_2,\ x:\ \tau \vdash e_2 \equiv_{\tau_1} e_3}{x:\ \tau \vdash e_1 \equiv_{\tau_1} e_3}$

4. congr $\dfrac{x:\ \tau \vdash e_1 \equiv_{\tau_1} e_2}{x:\ \tau \vdash p(e_1) \equiv_{\tau_2} p(e_2)}\quad p:\ \tau_1 \longrightarrow \tau_2$

5. E.x $\dfrac{\vdash \tau \text{ type}}{x:\ \tau \vdash x \downarrow \tau}$

6. E.congr $\dfrac{x:\ \tau \vdash e_1 \equiv e_2,\ x:\ \tau \vdash e_1 \downarrow \tau_1}{x:\ \tau \vdash e_2 \downarrow \tau_1}$

7. subst $\dfrac{x:\ \tau \vdash e \downarrow \tau_1,\ x:\ \tau_1 \vdash \phi}{x:\ \tau \vdash [e/x]\phi}$

8. $[-].\xi$ $\dfrac{x:\ \tau \vdash e_1 \equiv_{\tau_1} e_2}{x:\ \tau \vdash [e_1] \equiv_{T\tau_1} [e_2]}$

9. $E.[-]$ $\dfrac{x:\ \tau \vdash e_1:\ \tau_1}{x:\ \tau \vdash [e_1] \downarrow T\tau_1}$

10. $\mu.\xi$ $\dfrac{x:\ \tau \vdash e_1 \equiv_{T\tau_1} e_2}{x:\ \tau \vdash \mu(e_1) \equiv_{\tau_1} \mu(e_2)}$

11. $\mu.\beta$ $\dfrac{x:\ \tau \vdash e_1 \downarrow \tau_1}{x:\ \tau \vdash \mu([e_1]) \equiv_{\tau_1} e_1}$

12. $\mu.\eta$ $\dfrac{x:\ \tau \vdash e_1 \downarrow T\tau_1}{x:\ \tau \vdash [\mu(e_1)] \equiv_{T\tau_1} e_1}$

13. let.$\xi$ $\dfrac{x:\ \tau \vdash e_1 \equiv_{\tau_1} e_2,\ x':\ \tau_1 \vdash e_1' \equiv_{\tau_2} e_2'}{x:\ \tau \vdash (\text{let}x' \Leftarrow e_1\text{in}e_1') \equiv_{\tau_2} (\text{let}x' \Leftarrow e_2\text{in}e_2')}$

14. unit $\dfrac{x:\ \tau \vdash e_1:\ \tau_1}{x:\ \tau \vdash (\text{let}x_1 \Leftarrow e_1\text{in}x_1) \equiv_{\tau_1} e_1}$

15. ass $\dfrac{x:\tau\vdash e_1:\tau_1,\ x_1:\tau_1\vdash e_2:\tau_2,\ x_2:\tau_2\vdash e_3:\tau_3}{\begin{array}{c}x:\tau\vdash(\text{let }x_2\Leftarrow(\text{let }x_1\Leftarrow e_1\text{in}e_2)\text{ in }e_3)\\ \equiv_{\tau_3}(\text{let }x_1\Leftarrow e_1\text{ in }(\text{let }x_2\Leftarrow e_2\text{in }e_3))\end{array}}$

16. let.$\beta$ $\dfrac{x:\ \tau\vdash e_1\downarrow\tau_1,\ x_1:\ \tau_1\vdash e_2:\tau_2}{x:\ \tau\vdash(\text{let}x_1\Leftarrow e_1\text{in}e_2)\equiv_{\tau_2}[e_1/x]e_2}$

17. let.$p$ $\dfrac{x:\ \tau\vdash e_1:\ \tau_1}{x:\ \tau\vdash p(e_1)\equiv_{\tau_1}(\text{let}x_1\leftarrow e_1\text{in}p(x_1))}$

$$p:\ \tau_1\to\tau_2$$

简单程序语言的一个理论是由一组对以上推理规则封闭的等价方程和存在论断构成的集合 $\mathcal{T}$. 对于理论 $\mathcal{T}$ 可以同简单一般语言一样地定义一个相应的范畴 $\mathcal{F}(\mathcal{T})$.$\mathcal{F}(\mathcal{T})$ 对应于一个 Kleisli triple $(T,\eta,_^*)$, 且 $\eta$ 满足单射要求. 这样使得理论 $\mathcal{T}$ 正是满足在 $\mathcal{F}(\mathcal{T})$ 中规范解释的这组等价方程和存在论断.

简单程序语言对应于在范畴内的解释是 sound 和 complete. 证明与简单一般语言的情况相同.

## 参考文献


1 MacLane S. Categories for the Working Mathematician. Heidelberg: Springer–Verlag, 1971

2 Moggi E. Notions of computation and monads. Information and Computation, 1991, 93: 55~92

# 第 18 章

## 综合微分几何

微分几何是研究微分流形上的几何性质的数学，是服务于连续力学 (continuum mechanics) 的数学.

17 世纪牛顿，莱布尼兹发明了微积分，为研究物体的连续运动提供了计算工具. 牛顿是把微积分运算直接作为代数运算的，当时并没有极限的概念. 极限的概念是后来人们为了严格化微积分理论而引入的，极限概念成为现代微积分理论的基础，微分积分的概念全都用极限的语言来定义.

微分流形的引入是数学物理学进一步发展的需要，微分积分的运算需要空间是平直的，即具有一向量空间的结构，从而有流形局部平直化的程序： atlas- 流形上的每一点有一开邻域同胚于欧氏空间的一个开球. 但是 atlas 使流形上的微积分计算变成一个非常复杂的程序. 微分流形以及它们之间的连续可微映射构成一个范畴. 但是这个范畴缺乏一些应有的好性质，例如不存在函数空间. 这样使得在这个范畴内分析问题，实行计算变得很困难甚至不可能.

60 年代， Lawvere 提出 categorical dynamics 的概念，把无穷小直接作为计算对象，公理化流形范畴，使非平直空间上的直接微

分积分运算成为可能.

A. Kock 进一步深化具体化这一思想, 从而有综合微分几何学 (synthetic differential geometry)[4].

综合微分几何是公理化的. $\mathcal{E}$ 是光滑空间与光滑空间之间的光滑映射 (可以是无穷可微函数) 的范畴, 一个物体 $B$ 由于有内聚性, 所以不能只用它的原子 $b: 1 \longrightarrow B$ 的堆积来刻画, 而需要尺寸不同的"颗粒"或图形 (figure) 来描述, $x: X \longrightarrow B$. 所以在 $\mathcal{E}$ 中的 $B$ 的元素的概念是指以 $B$ 为 codomain 的任一 $\mathcal{E}$ 中的映射 $X \longrightarrow B$,$X$ 称为 domain of variation. 记 $x \in B$. 以 $B$ 为 codomain 的映射称为 $B$ 的一个推广了的元素 (generalized element). 这样在范畴 $\mathcal{E}$ 中我们可以方便地运用元素的概念来定义不同的结构, 就像在一般以集合论为基础的数学中一样. 只是有一点我们需要注意, $\mathcal{E}$ 中的逻辑不是经典的二值逻辑, 而是所谓的直觉主义逻辑 (intuitionistic logic), 所以如选择公理, 排中律, 反证法等在 $\mathcal{E}$ 中不适用.

范畴 $\mathcal{E}$ 具有卡氏积, 并且,

**公理 1** $\mathcal{E}$ 是卡氏积封闭的 (cartesian closed), 即函数空间存在.

这就是说, 对 $\mathcal{E}$ 中任一对象 $X$, 卡氏积函子 $X \times _: \mathcal{E} \longrightarrow \mathcal{E}$ 具有一个 right adjoint, 函数空间函子 $(\ )^x: \mathcal{E} \longrightarrow \mathcal{E}$.

$$\frac{X \times Y \longrightarrow Z}{Y \longrightarrow Z^X}$$

这里 $Y,Z$ 是 $\mathcal{E}$ 中对象, $X \times Y$ 到 $Z$ 的映射 $X \times Y \longrightarrow Z$ 一一自然对应于 $Y$ 到 $Z^X$ 的映射 $Y \longrightarrow Z^X$,$Z^X$ 即是 $X$ 到 $Z$ 的函数空间.

函数空间的存在对物理模型的分析计算是必要的. 例如为描述物体 $B$ 在空间 $E$ 中的运动, 让 $T$ 为一维空间代表时间, 物体 $B$ 的运动可以由映射 $f: T \times B \longrightarrow E$ 来描述. 对时刻 $t$, 以及 $B$ 上

的一点 $b$, $f(t,b)$ 给出在时刻 $t$, 点 $b$ 在 $E$ 中的位置. 若空间 $E$ 有一度量 $d$: $E\times E\longrightarrow E$, $e_0$ 为 $E$ 中一点, 那么映射的复合

$$\begin{array}{ccc} T\times B & \xrightarrow{f} & E \\ & \searrow^{d(e_0,-)\circ f} & \downarrow d(e_0,-) \\ & & E \end{array}$$

给出 $B$ 上任一点 $b$ 在任一时刻 $t$ 到 $e_0$ 点的距离

若固定点 $b$, $f(_,b)$ 给出 $b$ 点的运动轨迹. 即有 $\overline{f}$: $B\longrightarrow E^T$. 这里 $\overline{f}(b)=f(_,b)$. $E^T$ 是轨迹空间, 它独立于物体 $B$ 而存在. 因为 $E$ 是一平直空间, 所以它有一向量空间结构, 记为 $V$. 从 $E^T$ 到 $V^T$ 有一映射 $\dot{(\ )}$: $E^T\longrightarrow V^T$. $\overline{f}$ 与 $\dot{(\ )}$ 的复合

$$\begin{array}{ccc} B & \xrightarrow{\overline{f}} & E^T \\ & \searrow^{\dot{\overline{f}}} & \downarrow \dot{(\ )} \\ & & V^T \end{array}$$

给出在运动 $f$ 中 $B$ 上任一点的运动速度.

同样, 若固定时刻 $t$, $f(t,_)$: $B\longrightarrow E$ 给出从 $B$ 到 $E$ 的一个映射, 即给出 $B$ 在空间 $E$ 中的一个 placement. 这样我们有如下映射

$$\overline{\overline{f}}:\ T\longrightarrow E^B,\quad \overline{\overline{f}}(t)=f(t,_).$$

函数空间 $E^B$ 是 $B$ 的 placement 的空间, 它独立于时间 $T$ 而存在. 若物体 $B$ 的质量为 $\mu(B)$, 那么 $\overline{\overline{f}}$ 与映射 $\frac{1}{\mu(B)}\int\limits_B(\ )d\mu$: $E^B\longrightarrow E$ 的复合给出相应于运动 $f$ 的物体 $B$ 的重心.

$\mathcal{E}$ 包含几何线 $R$. 当我们取定 $R$ 上的两点 0,1, 以从 0 到 1 的距离为标准尺可以确定别的线段的长度. 线段在平面上的移动给

出加法，用直尺和圆规构造长度与已给二线段的长度成比例的第三条线段，给出乘法，这样 $R$ 成为一个可换环， $R$ 的数学模型即为实数环 $\mathbf{R}$.

$f,g:\ R^n \longrightarrow R^m$ 是 $\mathcal{E}$ 中的映射，这里 $n$, $m$ 均为正整数， $A$ 是 $f$, $g$ 的 equalizer

$$A \hookrightarrow R^n \underset{g}{\overset{f}{\rightrightarrows}} R^m$$

我们称 $A$ 为一个代数簇 (algebraic variety). 例如单位圆 $S^1$ 就是一个 equalizer,

$$S^1 \hookrightarrow R^2 \underset{g}{\overset{f}{\rightrightarrows}} R^1$$

$f(x,y)=x^2+y^2$, $g(x,y)=1$; 单位球面 $S^2$ 也是这样的代数簇

$$S^2 \hookrightarrow R^3 \underset{g}{\overset{f}{\rightrightarrows}} R$$

$f(x,y,z)=x^2+y^2+z^2$, $g(x,y,z)=1$.

可以认为范畴 $\mathcal{E}$ 是由这样的代数簇生成的. 特别无穷小空间 $D$ 是这样一个代数簇:

$$D \hookrightarrow R^2 \underset{O}{\overset{x^2}{\rightrightarrows}} R.$$

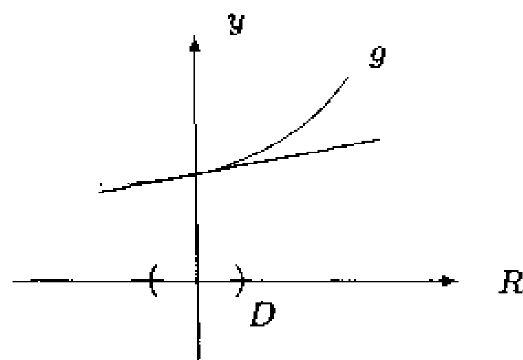
仿射 scheme 局部为代数簇.

一阶无穷小空间 $D=\{x\in R|x^2=0\}$, $0\in D$, 因为 $\mathcal{E}$ 中的逻辑不是二值的， $D$ 中含有其他非零元素.

**公理 2** $D$ 到 $R$ 的任一映射 (在 $\mathcal{E}$ 中)$g:\ D\longrightarrow R$ 是线性的. 即存在唯一 $b\in R$, 使得 $g(d)=g(0)+d\cdot b$.

公理 2 是说无穷小空间 $D$ 充分小，小到在 $D$ 上的任一函数

都是线性的；但又足够大，大到每一直线的斜率可以唯一确定.




注意，$g$ 可以是从 $R$ 的包含 $D$ 的一个子集到 $R$ 的映射，$b$ 是 $g$ 的斜率，即 $g$ 在 0 点的导数，记为 $b = g'(0)$.

由公理 2 中 $b$ 的唯一性，可知 $D$ 中元素具有消去律，若 $\forall d \in D$, $d \cdot b_1 = d \cdot b_2$, 那么 $b_1 = b_2$.

$D$ 上具有 $R$- 乘法；对于 $r \in R, d \cdot r \in D$. 这是因为 $(d \cdot r)^2 = d^2 \cdot r^2 = 0 \cdot r^2 = 0$. 但是对 $d_1, d_2 \in D$、$d_1 + d_2 \in D$ 当且仅当 $d_1 \cdot d_2 = 0$.

定义从 $R \times R$ 到 $R^D$ 的映射 $\alpha$： $R \times R \longrightarrow R^D$. $\alpha(a,b)(d) = a + d \cdot b$. 公理 2 说明 $\alpha$ 的逆存在.

在 $R \times R$ 上定义对偶数环 (ring of dual numbers) 的乘法 $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1a_2 + b_2a_1)$. 这样 $R \times R$ 成为一个 $R$-代数. 记这一 $R$- 代数为 $R[\varepsilon]$, 那么 $\alpha$ 成为 $R$- 代数同态，易见 $\alpha$ 保持加法与 $R$ 的数乘，$\alpha$ 也保持 $R[\varepsilon]$ 的乘法：$\alpha$ : $R[\varepsilon] \longrightarrow R^D$,

$$\begin{aligned}\alpha((a_1, b_1) \cdot (a_2, b_2))(d) &= \alpha(a_1a_2, b_1a_2 + b_2a_1)(d) \\ &= a_1a_2 + d \cdot (b_1a_2 + b_2a_1),\end{aligned}$$

而

$$\begin{aligned}\alpha(a_1, b_1)(d) \cdot \alpha(a_2, b_2)(d) &= (a_1 + db_1) \cdot (a_2 + db_2) \\ &= a_1a_2 + d(b_1a_2 + b_2a_1) + d^2b_1b_2 \\ &= a_1a_2 + d(b_1a_2 + b_2a_1)\end{aligned}$$

这是因为 $d^2 = 0$.

这样，公理 2 可以解释为：作为 $R$- 代数 $R^D$ 同构于对偶数环 $R[\varepsilon]$.

$\Pi_1,\Pi_2$ 分别是乘积空间 $R\times R$ 到它的第一，第二分量空间的投影， $\Pi_1,\Pi_2$ 与 $\alpha^{-1}$ 的合成给出从 $R^D$ 到 $R$ 的两个 $R$- 线性映射，对于 $g\in R^D$, $g=db$

$\beta=\Pi_1\circ\alpha^{-1}:\ R^D\longrightarrow R,\quad \beta(g)=g(0)$

$\gamma=\Pi_2\circ\alpha^{-1}:\ R^D\longrightarrow R,\quad \gamma(g)=b$, 为 $g$ 的斜率 ($g$ 在 0 点的导数).

在范畴 $\mathcal{E}$ 中经典逻辑不成立，以下的例子说明排中律将导致矛盾.

由排中律定义函数 $g:\ D\longrightarrow R$,

$$g(d)=\begin{cases}1, & 若\quad d\neq 0,\\ 0, & 若\quad d=0.\end{cases}$$

公理 2 在 $\mathcal{E}$ 中成立，所以 $D\neq\{0\}$, 那么由排中律可以取 $d_0\in D, d_0\neq 0$, 由公理 2, $g(d)=g(0)+d\cdot b$, 特别，$g(d_0)=g(0)+d_0b$, 由 $g$ 的定义有 $1=d_0b$. 平方等式两侧，我们得到 $1=d_0^2b^2=0$.

综合微分几何的逻辑是 constructive, 或称 intuitionistic. 我们用 〚 〛 表示满足某一性质的 $\mathcal{E}$ 的某一对象的子对象，以区别于子集的符号 $\{\ \}$.

下面我们要用公理 2 去定义函数 $f:\ R\longrightarrow R$ 在 $R$ 上任一点 $x$ 的导数，以及推导相应的导数的运算性质. (我们称 $\mathcal{E}$ 中以 $R$ 为 codomain 的映射为函数.)

**定义 1** $f:\ R\longrightarrow R, x\in R$. 让 $g(d)=f(x+d)$, 那么 $g$ 是一个映射 $g:\ D\longrightarrow R$. 由公理 2 $f(x+d)=f(x)+db$. 记 $b=f'(x)$, 那么 $f(x+d)=f(x)+df'(x)$.

这样 $f'$ 定义在 $R$ 的每一点上，即 $f'$ 是 $R$ 到 $R$ 的一个函数. 若 $f$ 只是定义在 $R$ 的一个子集 $U$ 上，让 $U'=$ 〚 $x\in U|x+d\in U,\forall d\in D$ 〛 $\subseteq U$, 那么 $f'$ 是 $U'$ 到 $R$ 的函数.

**定理 1** $f, g: U \longrightarrow R$, $r \in R$, 那么

1. $(f+g)' = f' + g'$
2. $(rf)' = rf'$
3. $(fg)' = f'g + fg'$
4. 若 $g: V \longrightarrow U$, $f: U \longrightarrow R$, $(f \circ g)' = (f' \circ g)g'$
5. $1'_R = 1$, $1_R$ 是 $R$ 到自身的恒等映射.
6. $r' = 0$, $r$ 是值为 $r$ 的常量函数.

**证明**

1.

$$
\begin{aligned}
(f+g)(x+d) &= (f+g)(x) + d(f+g)'(x) \\
&= (f(x)+g(x)) + d(f+g)'(x)
\end{aligned}
$$

又有

$$
\begin{aligned}
(f+g)(x+d) &= f(x+d) + g(x+d) \\
&= (f(x) + df'(x)) + (g(x) + dg'(x)) \\
&= (f(x)+g(x)) + d(f'(x) + g'(x))
\end{aligned}
$$

于是有 $d(f+g)'(x) = d(f'(x)+g'(x)), \forall d \in D$. 由消去律，我们有 $(f+g)'(x) = f'(x) + g'(x)$.

2. 留作练习.

3.

$$
\begin{aligned}
(f \cdot g)(x+d) &= (f \cdot g)(x) + d(f \cdot g)'(x) \\
&= (f(x)g(x)) + d(f \cdot g)'(x)
\end{aligned}
$$

又有

$$
\begin{aligned}
(f \cdot g)(x+d) &= f(x+d)g(x+d) \\
&= (f(x) + df'(x))(g(x) + dg'(x)) \\
&= f(x)g(x) + d(f'(x)g(x) + f(x)g'(x)) + d^2 f'(x)g'(x) \\
&= f(x)g(x) + d(f'(x)g(x) + f(x)g'(x))
\end{aligned}
$$

这样 $d(fg)'(x)=d(f'(x)g(x)+f(x)g'(x)), \forall d\in D$. 所以 $(fg)'(x)=f'(x)g(x)+f(x)g'(x)$.

4. $f\circ g(x+d)=f\circ g(x)+d(f\circ g)'(x)$, 而

$$\begin{aligned}f\circ g(x+d)&=f(g(x+d))\\&=f(g(x)+dg'(x))\quad \text{注意 } dg'(x)\in D\\&=f(g(x))+dg'(x)\cdot f'(g(x)),\end{aligned}$$

这样 $d(f\circ g)'(x)=dg'(x)f'(g(x)), \forall d\in D$. 所以 $(f\circ g)'(x)=f'(g(x))g'(x)=(f'\circ g)(x)g'(x)$.

5. 留作练习

6. $r(x+d)=r=r+d\cdot 0$, 又有 $r(x+d)=r(x)+dr'(x)=r+dr'(x)$, 所以 $r'=0$.

对于二元函数, 可以如下定义偏导数.

**定义 2** $f:\mathbf{R}^2\longrightarrow\mathbf{R}$, $r_1, r_2\in\mathbf{R}$.

让 $g(d)=f(r_1+d,r_2)$, 由公理 2 存在唯一 $b$, $g(d)=g(0)+db$, 记 $b=\dfrac{\partial f}{\partial x_1}(r_1,r_2)$, 即有 $f(r_1+d,r_2)=f(r_1,r_2)+d\dfrac{\partial f}{\partial x_1}(r_1,r_2)$. 可以同样定义 $\dfrac{\partial f}{\partial x_2}(r_1,r_2)$.

不难证明

$$\begin{aligned}f(r_1+d_1,r_2+d_2)=f(r_1,r_2)&+d_1\frac{\partial f}{\partial x_1}(r_1,r_2)\\&+d_2\frac{\partial f}{\partial x_2}(r_1,r_2)+d_1d_2\frac{\partial^2 f}{\partial x_1\partial x_2}(r_1,r_2),\end{aligned}$$

这里 $\dfrac{\partial^2 f}{\partial x_1\partial x_2}(r_1,r_2)=\dfrac{\partial}{\partial x_1}(\dfrac{\partial f}{\partial x_2})$. 由公理 2 中导数存在的唯一性, 可见 $\dfrac{\partial^2 f}{\partial x_1\partial x_2}=\dfrac{\partial^2 f}{\partial x_2\partial x_1}$

**练习** 若 $\tau: D\times D\longrightarrow R$ 具有性质 $\tau(d,0)=\tau(0,d)=\tau(0,0)$, $\forall d\in D$, 那么存在唯一 $t: D\longrightarrow R$, 且 $\tau(d_1,d_2)=t(d_1d_2)$.

**公理 2'** (公理 2 的延伸)

对任意 $k=1,2,\cdots$, $g: D_k \longrightarrow R$, 存在唯一 $b_1,\cdots,b_k \in R$, 使得 $\forall d \in D$, $g(d)=g(0)+\sum_{i=1}^{k} d^i b_i$. 这里 $D_k$ 是 $k$ 阶无穷小空间 $D_k=\{x \in R | x^{k+1}=0\}$.

这样可以推出对任一 $f: R \longrightarrow R$, $x \in R$, $f$ 的 $k$- 阶 Taylor 级数存在:

$$f(x+d)=f(x)+df'(x)+\cdots+\frac{d^k}{k!}f^{(k)}(x+\varepsilon_k), \quad d \in D_k.$$

$D=D_1$ 是一阶无穷小空间, 定义

$$D_k(n)=\big\{(x_1,x_2,\cdots,x_n) \in R^n | x_1,x_2,\cdots,x_n \text{ 中任意 } k+1 \text{ 个元素的乘积为 } 0\big\}, \quad k<n.$$

显然我们有 $D_k(n) \subseteq D_k^n$. 我们记 $D_1(n)=D(n)$, 特别 $D(2) \subseteq D^2$.

**公理 2 的另一形式**: $D_k(n)$ 到 $R$ 的任一映射是一多项式, 具有次数 $\leqslant k$.

$l_i: D \longrightarrow D(n)$, $l_i(d)=(0,\cdots,d,\cdots,0)$, d 在第 $i$ 个位置上,

$\Delta: D \longrightarrow D(n)$, $\Delta(d)=(d,d,\cdots,d)$.

**定义 3** $M$ 是 $\mathcal{E}$ 中空间, $M$ 称为无穷小线性的 (infinitesimally linear), 若对任一组 $n$ 个 $(n=2,3,4,\cdots)$ 映射 $t_i: D \longrightarrow M$, $t_1(0)=\cdots=t_n(0)$. 则存在唯一 $t: D(n) \longrightarrow M$, $ti=t \circ l_i$.

**命题 1** $R$ 是无穷小线性的

**证明** 给出 $t_i: D \longrightarrow R$, $i=1,2,\cdots,n$. 并且 $t_1(0)=\cdots=t_n(0)=a$. 由公理 2, $t_i(d)=a+db_i$. 定义 $t: D(n) \longrightarrow R$ 如下, $t(d_1,\cdots,d_n)=a+d\sum d_i b_i$, 则有 $t_i=t \circ l_i$. 关于 $l$ 的唯一性, 设还有 $s: D(n) \longrightarrow R$, $s \circ l_i=t_i$. 由公理 2 的另一形式, $s(d_1,\cdots,d_n)=a+\sum d_i a_i$. 由于 $s \circ l_i=t_i$, 有 $a_i=b_i$, 所以 $s=t$.

**定义 4** $M$ 是一个空间，比如可以是 $R$, $R^n$ 或 $R^n$ 的任一仿射 scheme. $x$ 是 $M$ 上的任一点， $M$ 上以 $x$ 为基点的一个切向量 $t$ 定义为从 $D$ 到 $M$ 的一个映射 $t:\ D \longrightarrow M, t(0)=x$.

这个定义与流形上的切向量的定义是一致的：流形 $M$ 上点 $x$ 的一个切向量是经过 $x$ 的极短曲线的一个等价类.

函数空间 $M^D$ 可以看为是 $M$ 上所有切向量构成的空间. $M^D$ 称为 $M$ 的 tangent bundle. 从 $M^D$ 到 $M$ 有一自然投影 $\Pi:\ M^D \longrightarrow M$, 若切向量 $t$ 的基点 $t(0)=x$, 那么 $\Pi(t)=x$. 这样点 $x$ 上的纤维 $\Pi^{-1}(x)=M^D_x$, 称为 $M$ 在 $x$ 点的切向量空间.

**命题 2** 若 $M$ 是无穷小线性的， $M^D_x$ 有如下向量空间结构：$r \in R$, $t_1, t_2 \in M^D_x$.

定义数乘 $rt_1(d)=t_1(rd)$.

对于 $t_1, t_2:\ D \longrightarrow M$, 由 $M$ 的无穷小线性，存在唯一的 $t:\ D(2) \longrightarrow M$ 使得 $t_1 = t \circ l_1:\ D \longrightarrow D(2) \longrightarrow M, t_2 = t \circ l_2:\ D \longrightarrow D(2) \longrightarrow M$.

定义 $(t_1+t_2)(d)=t \circ \Delta:\ D \longrightarrow D(2) \longrightarrow M$. 这里 $\Delta$ 是对角线映射，即有 $(t_1+t_2)(d)=t(d,d)$.

如上定义的加法是可结合的和可换的， $R$ 数乘与加法是可分配的，详细证明请参阅 [4] p.35.

$M$ 上的切向量可以表示为从 $D$ 到 $M$ 的映射 (represented by $D$). 这样可以简化不少概念的理解与运算，例如向量场 (vector field).

$M$ 上的一个向量场，或 $M$ 上的一个一阶常微分方程是一个由 $M$ 到 $M^D$ 的映射 $F:\ M \longrightarrow M^D$, 具有性质 $\Pi \circ F = 1_M$, 就是说 $F(m)(0)=m, \forall m \in M$.

由于 $\mathcal{E}$ 是卡氏积闭合的， $F$ 相当于 $\overline{F}:\ M \times D \longrightarrow M$, $\overline{F}(m,0)=m$; $F$ 又相当于 $\check{F}:\ D \longrightarrow M^M$, $\check{F}(0)=1_M$.

$$\frac{\dfrac{F : M \longrightarrow M^D}{\overline{F} : M \times D \longrightarrow M}}{\check{F} : D \longrightarrow M^M}$$

$M$ 上的一个流 (flow) 是一个由 $M \times R$ 到 $M$ 的映射，这里 $R$ 只取加群结构，这样 $M$ 的一个向量场 $F$ 可以看为 $M$ 上的一个无穷小流 (infinitesimal flow)．而对于一个流 $M \times R \longrightarrow M$，限制其于 $D$ 上即是一个向量场．

两个向量场 $F, G$ 之间的映射 $f: F \longrightarrow G$，是一个从 $M$ 到 $M$ 的映射 $f: M \longrightarrow M$，使得以下图形可换

$$\begin{array}{ccc} M \times D & \xrightarrow{f \times 1_D} & M \times D \\ F \downarrow & & \downarrow G \\ M & \xrightarrow{f} & M \end{array}$$

对于一个固定的 $d \in D, \check{F}(d): M \longrightarrow M$ 称为 $M$ 的一个无穷小变换 (infinitesimal transformation).

**定理 2**　若 $M$ 是线性无穷小的，那么无穷小变换 $\check{F}(d): M \longrightarrow M$ 是一一的到上的 (bijection). $\check{F}(d)$ 的逆是 $\check{f}(-d)$.

**证明**　见 [4] p.40.

如果 $M$ 是线性无穷小的，那么 $M$ 上的向量场成为一个 $R^M$-模，让 $f \in R^M$, $F$ 是 $M$ 上一个向量场，因为 $F(m, _), G(m, _)$ 是向量空间 $M_m^D$ 中的向量，所以 $F(m, _) + G(m, _) = (F+G)(m, _)$ 仍是 $M_m^D$ 中的一个向量．

在 $M$ 的向量场上还可定义一个李乘法具有以下性质：

$$[F, G](m, d_1 d_2) = G(F(G(F(m, d_1), d_2), -d_1), -d_2),$$

$$[F, G] = -[G, F].$$

于是 $M$ 上的向量场构成一个 $R$- 李代数.

空间 $M$ 上的 tangent bundle 可以由从 $D$ 的映射来代表是综合微分几何学的特点之一, 它的另一个特点是 tangent bundle 函子 $(\ )^D$ 有一个 right adjoint $(\ )_D$

$$\frac{X^D \longrightarrow Y}{X \longrightarrow Y_D}$$

这样可以使有关积分, form 与 current 的很多计算得以简化.

## 参考文献


1 Lawvere F W. Categorical dynamics. Topos Theoretic Methods in Geometry, Aarhus: Mat. Inst. Aarhus Univ., 1979, 1~28

2 Lawvere F W. Toward the description in a smooth topos of the dynamically possible motions and deformations of a continuous body. Cahiers Topologie Géom Différentielle, 1980, 21: 377~392

3 Lawvere F W. Introduction to categories in continuum physics. Lecture Notes in Math., 1986, 1174: 1~16

4 Kock A. Synthetic Differential Geometry. Cambridge: Cambridge Univ. Press, 1981

# 第 19 章

# Sheaf 理论与代数几何

$X$ 是一个拓扑空间. 以 $X$ 为连续参变量的一组空间是空间 $X$ 上的一种数学结构. 这种数学结构与保持此结构的映射构成一个范畴. 这种 $X$ 上空间的范畴具有很多与空间 $X$ 相对应的性质. 因此对此种范畴的研究理解可以帮助对空间 $X$ 本身的研究与理解, 反之亦然.

空间 $X$ 上的 sheaf 组成的范畴正是这样一种以 $X$ 为连续参变量的空间的范畴. sheaf 范畴又具有其自身的很多性质.

在这一章里首先介绍 sheaf 理论; 其次介绍 sheaf 上的上同调; 最后是代数几何: 古典代数几何的主要概念理论, 以及 scheme, sheaf 的上同调在代数几何中的应用.

## § 1 Sheaf 理论

Sheaf 是一种数学结构, 它可以把一个空间上的局部信息合理地粘连在一起, 成为全部, 整体的信息. 以下这个典型例子可以告诉我们 sheaf 思想的一种起源.

$X$ 是一个拓扑空间, $U$ 是 $X$ 的任一开子集. 令 $F(U)$ 为 $U$ 上连续复值函数的集合. $\{U_i\}_{i\in I}$ 是 $U$ 的一个开复盖. 我们知

道，若一族函数 $\{f_i\}_{i\in I}$, $f_i\in F(U_i)$, 满足条件：对任意 $i,j\in I$, $f_i\big|_{U_i\cap U_j}=f_j\big|_{U_i\cap U_j}$ ($f_i\big|_{U_i\cap U_j}$ 是 $f_i$ 在 $U_i\cap U_j$ 上的限制), 那么可以将 $\{f_i\}_{i\in I}$ 扩展到 $U$ 上的一个连续复值函数 $f$, 具有性质 $f\big|_{U_i}=f_i$. 这样的 $F$ 是 $X$ 上的一个 sheaf.

让 $O(X)$ 表示拓扑空间 $X$ 的开集的集合. $O(X)$ 做成一个 poset $(O(X),\subseteq)$,(偏序集是一个集合具有一个二元关系 $\leqslant$, 这一二元关系满足

(1) 自反性，$x\leqslant x$;

(2) 反对称性，若 $x\leqslant y, y\leqslant x$, 那么 $x=y$;

(3) 传递性，$x\leqslant y, y\leqslant z$, 那么 $x\leqslant z$.

Poset 只要求 (1),(3). $(O(X),\subseteq)$ 构成一个偏序集，(但这里我们只用到它是一个 poset.) 因而可以将 $(O(x),\subseteq)$ 看为一个范畴，因而有从 $(O(X),\subseteq)$ 到任一范畴，例如集合的范畴 $S$ 的反变函子范畴 $S^{(O(X),\subseteq)^{\mathrm{op}}}$. 我们按一般习惯将这个反变函子范畴记为 $S^{X^{\mathrm{op}}}$. $X$ 上的一个反变函子 $F$ 具有性质：若 $U\subseteq V\subseteq W$ 为 $X$ 的开子集，那么 $\rho_U^V: F(V)\longrightarrow F(U)$, $\rho_V^W: F(W)\longrightarrow F(V)$ 的合成 $\rho_V^W\circ\rho_U^V=\rho_U^W: F(W)\longrightarrow F(U)$. 反变函子范畴中的对象称为空间 $X$ 上的 presheaf.

**例 1** 常量函子 (constant presheaf)

让 $A$ 为一个固定的集合. 对 $X$ 的任一开集 $U$, 定义 $A(U)=A$. 若 $U\subseteq V$, 定义 $\rho_V^U=1_A: A(V)\longrightarrow A(U)$.

**例 2** 让 $Y$ 为另一拓扑空间. $U$ 是 $X$ 的任一开集，定义 $C^Y(V)$ 为由 $U$ 到 $Y$ 的连续函数的集合. 若 $U\subseteq V$, 那么 $\rho_V^U$: $C^Y(V)\longrightarrow C^Y(U)$, $f\longmapsto f\big|_U$.

**例 3** 让 $X$ 为 $\mathbf{R}^n$ 的一个开子集，定义 $C^1(U)$ 为 $U$ 上实值一阶可导函数的集合. 同样可以定义 $C^n$, $n=2,3,\cdots$.

**例 4** 让 $X$ 为 $\mathbf{C}^n$ 的一个开子集，$C^\infty(U)$ 为 $U$ 上复值解析函数.

**例 5** $X=\{0,1\}$ 为只含两个元素的离散空间. 定义 $P(X)=\{a,b\}$, $P(U)=\{a\}$. 若 $U\neq X$. 那么 $\rho_X^X=1_{\{a,b\}}$, $\rho_U^X$: $\{a,b\}\longrightarrow\{a\}$. $Q(X)=Q(\{0\})=\{a,b\}$, $Q(\phi)=Q(\{1\})=\{a\}$.

**定义 1** 空间 $X$ 上的 presheaf $F$ 是一个 sheaf, 若 $F$ 满足以下两个条件: $U$ 是 $X$ 的任一开集, $\{U_i\}_{i\in I}$ 为 $U$ 的任一开复盖.

(1) $s,t\in F(U)$, 若 $\rho_{U_i}^U(s)=\rho_{U_i}^U(t)$, $i\in I$, 那么 $s=t$.

(2) $\{s_i\}_{i\in I}$, $s_i\in F(U_i)$. 若 $\rho_{U_i\cap U_j}^{U_i}(s_i)=\rho_{U_i\cap U_j}^{U_j}(s_j)$, $\forall_{i,j\in I}$, 那么存在 $s\in F(U)$, 具有性质 $\rho_{U_i}^U(s)=s_i$.

Sheaf 之间的映射就是 sheaf 作为 presheaf 在 $S^{X^{op}}$ 之内的映射. 用 $\mathrm{Sh}(X)$ 表示 $X$ 上的 sheaf 以及它们之间的映射构成的范畴, $\mathrm{Sh}(X)$ 是 $S^{X^{op}}$ 的一个满 (full) 和忠实的 (faithful) 子范畴.

在以上例子中, $C^Y, C^1, C^2, \cdots, C^n, \cdots, C^\infty$ 均为 sheaf.

还有另一种方法定义 sheaf.

**定义 2** $U$ 为 $X$ 的任一开集, $\{U_i\}_{i\in I}$ 为 $U$ 的任一开复盖.

$$F(U)\xrightarrow{\ e\ }\prod_{i\in I}F(U_i)\ \underset{q}{\overset{p}{\rightrightarrows}}\ \prod_{(i,j)\in I\times I}F(U_i\cap U_j)$$

$$p((s_i)_{i\in I})=(\rho_{U_i\cap U_j}^{U_i}(s_i))_{(i,j)\in I\times I}$$
$$q((s_i)_{i\in I})=(\rho_{U_i\cap U_j}^{U_j}(s_i))_{(i,j)\in I\times I}$$
$$e(s)=(\rho_{U_i}^U(s))_{i\in I}.$$

若以上图形为一个 equalizer, 则说 $F$ 是 $X$ 上的一个 sheaf.

由 equalizer 的定义直接可证定义 1 与定义 2 等价

**定义 3** 一个 poset$(A,\leqslant)$ 为一个 directed set, 若对 $A$ 中任意两个元素 $a,b$, 存在 $c\in A$. 并且 $a\leqslant c$, $b\leqslant c$.

**例 6** 在 $O(X)$ 上定义新序 $U\leqslant V$ 当且仅当 $V\subseteq U$, 那么 $(O(X),\leqslant)$ 为一个 directed set.

**例 7** $U$ 是 $X$ 的一个开集，$x \in U.\{U_i^x | x \in U_i^x, U_i^x \subseteq U\}$ 应用例 6 中的序 $\leqslant$, $(\{U_i^x\}, \leqslant)$ 是一个 directed set.

**例 8** $F$ 为 $X$ 上的一个 presheaf, 定义 $F(U_i^x) \leqslant F(U_j^x)$ 当且仅当 $U_i^x \leqslant U_j^x$, 即有 $\rho_{U_j^x}^{U_i^x}: F(U_i^x) \longrightarrow F(U_j^x)$ 存在. 这样 $(\{F(U_i^x)\}, \leqslant)$ 是一个 directed set.

$U$ 是 $X$ 的一个开子集，$x \in U$, $(\{U_i^x\}_{i\in I}, \subseteq)$ 是 $(O(X), \subseteq)$ 的一个子 poset, 这样 $X$ 上的一个 presheaf $F$ 也是 $(\{U_i^x\}_{i\in I}, \subseteq)$ 上的一个反变函子.

**定义 4** 上极限 (colimit) $\varinjlim_{i\in I} F(U_i^x)$ 称为 $F$ 在 $x$ 点的 stalk, 记为 $\varinjlim_{i\in I} F(U_i^x) = F_x$. $F_x$ 中的元素称为 germ.

我们可以如下构造 stalk $F_x$ (用这种方法可以构造任一 direct set 的上极限).

首先构造 $\{F(U_i^x)\}_{i\in I}$ 的不交并 $\coprod_{i\in I} F(U_i^x)$. 然后在 $\coprod_{i\in I} F(U_i^x)$ 上定义一个二元关系 $u \sim v$ 当且仅当 $u \in F(U_i^x)$, $v \in F(U_j^x)$, 并且存在 $U_s^x$, $U_i^x \leqslant U_s^x$, $U_j^x \leqslant U_s^x$, $\rho_{U_s^x}^{U_i^x}(u) = \rho_{U_s^x}^{U_j^x}(v)$. 这就是说，若 $u$ 有关于 $v$, 则它们在某一阶段上 $(U_s^x)$ 相等. 二元关系 $\sim$ 满足自反性和对称性. 对于传递性：若 $u \sim v$, $v \sim w$, 即存在 $U_s^x$, $U_t^x$, $\rho_{U_s^x}^{U_i^x}(u) = \rho_{U_s^x}^{U_j^x}(v)$, $\rho_{U_t^x}^{U_j^x}(v) = \rho_{U_t^x}^{U_k^x}(w)$. 因为 $(\{F(U_i^x)\}_{i\in I}, \leqslant)$ 是一个 directed set, 所以存在 $U_z^x$, $F(U_s^x) \leqslant F(U_z^x)$, $F(U_t^x) \leqslant F(U_z^x)$, 使得 $\rho_{U_z^x}^{U_s^x}(\rho_{U_s^x}^{U_i^x}(u)) = \rho_{U_z^x}^{U_t^x}(\rho_{U_t^x}^{U_k^x}(w))$, 但这正是 $\rho_{U_z^x}^{U_i^x}(u) = \rho_{U_z^x}^{U_k^x}(w)$, 所以 $u \sim w$. 这就是说 $\sim$ 为一等价关系. 定义 $F_x = \coprod_{i\in I} F(U_i^x)/\sim$. 定义 $\tau_i: F(U_i^x) \longrightarrow F_x$ 为以下两个映射的合成，$F(U_i^x) \longrightarrow \coprod_{i\in I} F(U_i^x)$, $\coprod_{i\in I} F(U_i^x) \longrightarrow F_x$.

由以上构造直接可证以下命题成立.

**命题 1**

(1) $F_x$ 中每一个元素 $t_x$ 来自 $F(U)$, 这里 $U$ 是 $x$ 的某一邻域.

(2) $s_x, t_x \in F_x$, $s \in F(U)$, $t \in F(V)$. 那么 $s_x = t_x$ 当且仅当存在 $W \subset U \cap V$, 适合 $\rho^U_W(s) = \rho^V_W(t)$.

若 $f: F \longrightarrow G$ 是一个从 $F$ 到 $G$ 的自然变换. 对每一 $U^x_i$; $f_{U^x_i}: F(U^x_i) \longrightarrow G(U^x_i)$. 由上极限的定义, 我们有 $f_x$: $F_x = \varinjlim_{i\in I} F(U^x_i) \longrightarrow \varinjlim_{i\in I} G(U^x_i) = G_x$.

有关 stalk 的例子:

例 1 中的常量 presheaf $A$, $A_x = A$. 例 2, 例 3, 例 4 中的函数 sheaf $C^Y$, $C^1$, $C^\infty$ 的任一 germ $t_x$ 可以扩展为 $x$ 的某一开邻域上的一个函数. 例 5 中的 presheaf $P, Q, P_0, P_1$ 分别只含有一个元素; $Q_0 = \{a, b\}$, $Q_1$ 只含一个元素.

**命题 2** $F$ 是拓扑空间 $X$ 上的一个 sheaf. $U$ 是 $X$ 的一个开集. 若 $s, t \in F(U)$, $s = t$ 当且仅当 $s_x = s_t, \forall_x \in U$.

**证明** 充分性是显然的

必要性: 若 $s_x = t_x$, 则存在 $x$ 的一个开邻域 $U_x$ 使得 $\rho^U_{U_x}(s) = \rho^U_{U_x}(t)$, 这样 $\{U_x\}_{x\in U}$ 构成 $U$ 的一个开复盖, 由 sheaf 定义中的第一条, 我们有 $s = t$,

注意, 这一命题对 presheaf 不成立, 如例 5 中的 $P$.

下面我们要说明, $X$ 上的一个 sheaf 等同于以 $X$ 中的元素为连续参变量的 $X$ 上的一个空间

**定义 5** $X$ 是一个拓扑空间, $X$ 上的一个 sheaf 空间 $(E, p)$ 由一个拓扑空间 $E$ 以及由 $E$ 到 $X$ 的一个连续映射 $p$: $E \longrightarrow X$ 构成, 并且 $p$ 是一个局部同胚 (local bomeomorphism): 对任意 $y \in E$, 存在开集 $V, y \in V$, 及 $U$, $p(y) \in U$, 并且 $p|_V: V \longrightarrow U$ 是一同胚.

若 $(E', p')$ 为 $X$ 上另一 sheaf 空间, $(E, p)$ 到 $(E', p')$ 的一个映射 $f$ 是 $E$ 到 $E'$ 的一个连续映射, 并且 $p = p' \circ f$:

$$
\begin{array}{ccc}
E & \xrightarrow{f} & E' \\
& {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle p'} & \\
& X &
\end{array}
$$

这样 $X$ 上的 sheaf 空间，以及 sheaf 空间之间的映射构成一个范畴 $\mathrm{Shsp}(X)$.

$F$ 是 $X$ 上的一个 presheaf. 由 $F$ 我们可以造一个 $X$ 上的 sheaf 空间. 让 $LF = \coprod_{x\in X} F_x$, 这里 $\coprod_{x\in X} F_x$ 是 $F_x$ 的不交并. $p: LX \longrightarrow X$ 为自然射影. $LF$ 上的拓扑定义如下: $U$ 是 $X$ 的一个开集, $s \in F(U)$, 让 $\widehat{s}: U \longrightarrow LF, x \longmapsto s_x \in F_x, \widehat{s}(U) = \{s_x \in LF, x \in U\}$ 构成 $LF$ 的一组拓扑基: 若 $e \in \widehat{s}(U) \cap \widehat{t}(V)$, 那么 $e = s_x = t_x$, $x = p(e)$. 由命题 1, 存在 $x$ 的一个邻域 $W \subset U \cap V$, $\rho_W^U(s) = \rho_W^V(t)$, 即有 $\widehat{s}(W) = \widehat{t}(W)$ 为 $e$ 的一个基本开邻域. 自然射影 $\rho: LF \longrightarrow X$ 是连续的: 若 $U$ 是 $X$ 的一个开集, $p^{-1}(U) = \cup\{\widehat{s}(V)\}$, 这里 $s \in F(V)$, $V$ 是 $U$ 的开子集. 对任一 $e \in \widehat{s}(V)$, $\widehat{s}(U)$ 与 $U$ 同胚. 所以 $p$ 是一个局部同胚连续映射. 这样 $(LF, p)$ 构成 $X$ 上的一个 sheaf 空间.

若 $f: F \longrightarrow G$ 是 $F$ 到 $G$ 的一个自然变换, 对每一个 $x \in X$, $f_x: F_x \longrightarrow G_x$. 进而有

$$Lf = \coprod_{x\in X} f_x : LF = \coprod_{x\in X} F_x \longrightarrow \coprod_{x\in X} G_x = LG$$

这样 $L$ 是 $S^{X^{\mathrm{op}}}$ 到 $\mathrm{Shsp}(X)$ 的一个函子.

由 $X$ 上的一个 sheaf 空间 $(E,p)$, 我们可以构造 $X$ 上的一个 presheaf $TE$, $U$ 是 $X$ 的一个开子集, 定义 $TE(U) = \{$ 由 $U$ 到 $E$ 的连续函数, $\sigma: U \longrightarrow E$, 并且 $\rho\circ\sigma = 1_U\}$

$$\begin{array}{ccc} & \overset{\sigma}{\nearrow} & E \\ & & \downarrow p \\ U & \hookrightarrow & X \end{array}$$

若 $V \subseteq U$, 定义 $\rho_V^U$ : $TE(U) \longrightarrow TE(V)$, $\rho_V^U(\sigma) = \sigma|_V$.

**命题 3** $TE$ 是 $X$ 上的一个 sheaf.

证明 由连续函数的性质可证 $TE$ 满足 sheaf 定义中的条件.

**命题 4** $(E,p)$ 是一个 sheaf 空间, 那么 $(TE)_x = p^{-1}(x)$.

证明 $U$ 是包含 $x$ 的一个开集, $\{U_i^x\}$ 为 $U$ 内包含 $x$ 的开集集合. 我们有从 $TE(U_i^x)$ 到 $p^{-1}(x)$ 的映射

$$\begin{aligned} \tau_i:\ TE(U_i^x) &\longrightarrow p^{-1}(x) \\ \sigma &\longmapsto \sigma(x) \end{aligned}$$

并且有 $\tau_i = \tau_j \circ \rho_{U_j^x}^{U_i^x}$, 若 $U_j^x \subseteq U_i^x$.

如果存在另一个集合 $B$, 及 $TE(U_i^x)$ 到 $B$ 的一组映射
$b_i$: $TE(U_i^x) \longrightarrow B$, $b_i = b_j \circ \rho_{U_j^x}^{U_i^x}$. 我们希望有映射 $\tau$: $p^{-1}(x) \longrightarrow B$, 并且 $\tau \circ \tau_i = b_i$.

让 $e \in p^{-1}(x) \subseteq E$. 因为 $p$ 是局部同胚, 所以存在 $e$ 的一个开邻域 $W$, $p|_W$: $W \longrightarrow U_i^x$ 为一同胚. 那么 $(p|_W)^{-1}$ 是由 $U_i^x$ 到 $p^{-1}(x) \subseteq E$ 的一个连续映射,

$$\begin{array}{ccc} & \overset{(p|_W)^{-1}}{\nearrow} & E \\ & & \downarrow p \\ U_i^X & \hookrightarrow & X \end{array}$$

并且 $p \circ (p|_W)^{-1} = 1_{U_i^x}$.

定义 $\tau(e) = b_i(p|_W)^{-1}$. 若 $x \in V$, $p|_V$: $V \longrightarrow U_j^x$ 为另一同胚, 则有 $b_i((p|_W)^{-1}) = b_{ij}((p|_{W\cap V})^{-1}) = b_j((p|_V)^{-1})$, 这里 $b_{ij}$: $U_i^x \cap U_j^x \longrightarrow E$. 所以 $\tau$: $p^{-1}(x) \longrightarrow B$.

$$\begin{array}{ccc} p^{-1}(x) & \xrightarrow{\tau} & B \\ & \nwarrow_{\tau_i} \quad \nearrow_{b_i} & \\ & TE(U_i^X) & \end{array}$$

若 $\sigma: U_i^x \longrightarrow E, \rho\circ\sigma = 1_{U_i^x}$, 那么 $\tau\circ\tau_i\cdot(\sigma) = \tau(\tau_i(\sigma)) = \tau(\sigma(x)) = b_i(\sigma)$. $\tau$ 的唯一性是显然的. 由上极限的定义, 我们证明了 $(TE)_x = p^{-1}(x)$.

**推论** 若 $G \in S^{X^{op}}$, 那么 $(TLG)_x = G_x$.

**定理 1** $F$ 是 $X$ 上的 sheaf, 对 $X$ 的任开一子集 $U$, 有 $F(U) \approx TLF(U)$, 即 $F \approx TLF$.

**证明** 定义 $\alpha: F(U) \longrightarrow TLF(U)$

$$s \in F(U),\ \alpha(s) = \widehat{s},\ \widehat{s}(x) = s_x.$$

定义 $\beta: TLF(U) \longrightarrow F(U)$ 如下, $\sigma \in TLF(U)$, 即 $\sigma: U \longrightarrow LF$, 且 $p\circ\sigma = 1_U$, 那么 $\sigma(x) = t_x \in LF$, $t_x$ 具有一个基本开邻域 $\widehat{t^x}(U_x)$, $t^x \in F(U_x)$, $\sigma(x) = \widehat{t^x} = t_x^x$. $\{U_x\}_{x\in U}$ 构成 $U$ 的一个开复盖, 并且 $\rho^{U_x}_{U_x\cap U_y}(t^x) = \rho^{U_y}_{U_x\cap U_y}(t^y)$. 因为 $F$ 是 sheaf, 所以存在 $t \in F(U)$, $\rho^U_{U_x}(t) = t^x$, $t$ 是唯一的. 定义 $\beta(\sigma) = t$, 那么 $\widehat{t}(x) = t_x = \sigma(x)$, 即 $\widehat{t} = \sigma$. 我们有

$$\beta\circ\alpha(s) = \beta(\widehat{s}) = s,$$

$$\alpha\circ\beta(\sigma) = \alpha(t) = \widehat{t} = \sigma,$$

所以 $F(U) \approx TLF(U)$.

**推论** sheaf 的范畴 Sh($X$) 与 sheaf 空间的范畴 Shsp($X$) 等价 (equivalent).

Sheaf 空间正是以 $X$ 为连续参变量的 $X$ 上的空间, 它是用几何的方法去描述 sheaf, 很多时候可以给我们较为直观的对 sheaf 概念的理解.

在 presheaf 与 sheaf 之间, 我们有了一对函子

$$TL: S^{X^{op}} \longrightarrow \mathrm{Sh}(X) \quad i: \mathrm{Sh}(X) \longrightarrow S^{X^{op}}$$

这里 $i$ 是包含 (in clusion) 函子.

**定理 2** $TL$ 是 $i$ 的 left adjoint.

**证明** $F$ 是一个 sheaf, $G$ 是一个 presheaf. 自然变换 $\eta: G \longrightarrow iTL(G)$ 定义为 $\eta_U: G(U) \longrightarrow iTL(G)(U) = TL(G)(U)$, $\eta_U(s) = \widehat{s}$. 对 $f: G \longrightarrow F$, 定义 $\overline{f}: TL(G) \longrightarrow F$ 如下, $\overline{f}_U: TL(G)(U) \longrightarrow F(U)$, $\overline{f}_U(\sigma) = \beta \circ Lf \circ \sigma$. 这里 $Lf: LG \longrightarrow LF$, $\beta$ 是定理 1 中 $\alpha$ 的逆映射. 因为 $F$ 是 sheaf, 由定理 1, $TLF(U) \approx F(U)$. 若 $s \in G(U)$, 则有 $\overline{f}_U \circ \eta_U(s) = \overline{f}_U(\widehat{s}) = \beta \circ Lf \circ \widehat{s} = \beta(\widehat{f_U(s)}) = f_U(s)$.

若 $g: TLG \longrightarrow F$ 也满足 $g \circ \eta = f$. 由命题 4, $(TLG)_x = G_x$. 所以 $\eta_x: G_x \longrightarrow (TLG)_x$ 的逆 $\eta_x^{-1}$ 存在. $g_x = f_x \circ \eta_x^{-1}$ 是唯一确定的, 这就证明了 $\overline{f}$ 的唯一性.

$TL$ 通常称为 sheaf 化函子 (sheafification functor).

在代数几何中应用的 sheaf 不是取值于集合的范畴 $S$, 而是取值于可换群的范畴 Ab, 环的范畴 Ring, 或域 $K$ 上的代数的范畴 $K$-alg.

一般定义 sheaf 取值于范畴 Ah, 是由以可换群为值的 presheaf $\mathrm{Ab}^{X^{op}}$ 开始, 然后要求 presheaf 满足同样条件而成为 sheaf. 这里有另一种方法定义取值为可换群的 presheaf 或 sheaf.

首先, 某些符号

若 $f: A \longrightarrow B$, $g: C \longrightarrow D$, 我们记 $f \times g: A \times C \longrightarrow B \times D$ $f \times g(a, c) = (f(a), g(c))$.

若 $f: A \longrightarrow B$, $g: A \longrightarrow D$, 我们记 $(f, g): A \longrightarrow B \times D$, $(f, g)(a) = (f(a), g(a))$.

**定义 6** $C$ 是一个范畴, 具有有限乘积, 所以特别有 terminal 对象 1. $C$ 中的一个群对象 $C$ 是 $C$ 中的一个对象, 有 $C$ 中映射

$\mu: C \times C \longrightarrow C$ (乘法)

$e:\ 1 \longrightarrow C$ (单位元)

$(\ )^{-1}:\ C \longrightarrow C$ (逆运算)

满足

结合律

$\mu \circ (\mu \times 1_C) = \mu \circ (1_C \times \mu)$

(即 $(ab)c = a(bc)$)

$$\begin{array}{ccc} C \times C \times C & \xrightarrow{\mu \times 1_C} & C \times C \\ \downarrow 1_C \times \mu & & \downarrow \mu \\ C \times C & \xrightarrow{\mu} & C \end{array}$$

单位元

$\mu \circ (e, 1_C) = 1_C = \mu(1_C, e)$

$(ec = c = ce)$

$$\begin{array}{ccccc} C & \xrightarrow{(e,1_C)} & C \times C & \xleftarrow{(1_C,e)} & C \\ & \searrow 1_C & \downarrow \mu & 1_C \swarrow & \\ & & C & & \end{array}$$

逆元

$\mu \circ ((\ )^{-1}, 1_C) = e$

$= \mu \circ (1_C, (\ )^{-1})$

$(c^{-1}c = e = cc^{-1})$

$$\begin{array}{ccccc} C & \xrightarrow{((\ )^{-1},1_C)} & C \times C & \xleftarrow{(1_C,(\ )^{-1})} & C \\ \downarrow & & \downarrow \mu & & \downarrow \\ 1 & \xrightarrow{e} & C & \xleftarrow{e} & 1 \end{array}$$

若 $C$ 同时还满足可换律，则称 $C$ 为一个可换群对象.

可换律

$\mu = \mu \circ (p_2, p_1)$

$(ab = ba)$

$$\begin{array}{ccc} C \times C & \xrightarrow{(p_2,p_1)} & C \times C \\ & \mu \searrow \quad \swarrow \mu & \\ & C & \end{array}$$

这里 $p_1, p_2$: $C \times C \longrightarrow C$ 为自然射影.

$(D, \mu, (\ )^{-1}, e)$ 为另一群对象，那么 $C$ 到 $D$ 的一个群同态，$f$ 是 $C$ 中由 $C$ 到 $D$ 的一个映射，使得以下图形可换

$$\begin{array}{ccc} C\times C & \xrightarrow{f\times f} & D\times D \\ \mu\downarrow & & \downarrow\mu \\ C & \xrightarrow{f} & D \end{array} \qquad \begin{array}{ccc} 1 & \xrightarrow{e} & C \\ & \searrow^{e} & \downarrow f \\ & & D \end{array}$$

$$\mu\circ f\times f=f\circ\mu \qquad f\circ e=e$$

$$(f(a)f(b)=f(ab)) \qquad (f(e)=e)$$

这样 $\mathcal{C}$ 中的群对象以及它们之间的同态构成一个 $\mathcal{C}$ 的子范畴 $\mathrm{Grp}(\mathcal{C})$, 而可换群对象以及它们之间的同态构成 $\mathrm{Grp}(\mathcal{C})$ 的一个子范畴 $\mathrm{Ab}(\mathcal{C})$.

**定理 3** $\mathrm{Ab}(S^{X^{\mathrm{op}}})$ 等价于 $\mathrm{Ab}^{X^{\mathrm{op}}}$.

**证明** 让 $F\in\mathrm{Ab}(S^{X^{\mathrm{op}}})$. 对 $X$ 的任一开集 $U$ 有一组相应于定义 6 中可换图形，这样 $F(U)$ 是一个可换群. 因为 $\mu\colon F\times F\longrightarrow F$ 为一自然变换，所以对 $V\subseteq U$,

$$\begin{array}{ccc} F(U)\times F(U) & \xrightarrow{\mu_U} & F(U) \\ \rho_V^U\times\rho_V^U\downarrow & & \downarrow\rho_V^U \\ F(V)\times F(V) & \xrightarrow{\mu_V} & F(V) \end{array}$$

$\rho_V^U\circ\mu_V=\mu_V\circ(\rho_V^U\times\rho_V^U)$, 即 $\rho_V^U$ 为一群同态，$\rho_V^U: F(U)\longrightarrow F(V)$. 这样 $F$ 是一个取值为可换群的 $X$ 上的 presheaf.

反之，若 $G$ 是一个取值为可换群的 presheaf. 因为对 $V\subseteq U$, $\rho_V^U\colon G(U)\longrightarrow G(V)$ 是群同态. 用 $\mu_U,\mu_V$ 分别表示 $G(U)$ 与 $G(V)$ 的乘法，则有可换图形

$$\begin{array}{ccc} G(U)\times G(U) & \xrightarrow{\mu_U} & G(U) \\ \rho_V^U\times\rho_V^U\downarrow & & \downarrow\rho_V^U \\ G(V)\times G(V) & \xrightarrow{\mu_V} & G(V) \end{array}$$

这样 $\mu$ 是 $G\times G$ 到 $G$ 的自然变换.

同样可检验　单位元　　$e:\quad 1\longrightarrow G$

逆运算　$(\ )^{-1}:\quad G\longrightarrow G$

都是自然变换. 这样 $G$ 是 $S^{X^{\mathrm{op}}}$ 中的可换群对象, $G\in \mathrm{Ab}(S^{X^{\mathrm{op}}})$.

同样有 $\mathrm{Ab}(\mathrm{Sh}(X))$ 与以可换群为值的 sheaf 的范畴同构. 对于取值为环的 sheaf 也有相同的结果.

一个范畴 $C$ 具有有限乘积, 则可以定义 $C$ 中的代数结构, 如定义 6, 对于其他数学结构, $C$ 需要具有其他相应的性质.

下面是几个有关 sheaf, presheaf 的有用的性质.

**命题 5**　$F,G$ 是 $X$ 上的 presheaf, $f:\ F\longrightarrow G$ 为一自然变换. 那么

(1) 对 $X$ 的任一开集 $U$, $f_U:\ F(U)\longrightarrow G(U)$ 是一一的, 当且仅当 $f$ 是 $S^{X^{\mathrm{op}}}$ 中的 monomorphism, 即若有 $H\in S^{X^{\mathrm{op}}}$, 以及 $g,h:\ H\longrightarrow F$, 使得 $f\circ g=f\circ h$, 那么 $g=h$.

(2) $f_U:\ F(U)\longrightarrow F(V)$ 为满射, 当且仅当 $f$ 是 $S^{X^{\mathrm{op}}}$ 中的 epimorphism, 即若 $g,h:\ G\longrightarrow H$, $g\circ f=h\circ f$, 那么 $g=h$.

**命题 6**　$F,G$ 为 $X$ 上 sheaf, $f:\ F\longrightarrow G$ 是自然变换. 那么, 对 $X$ 上任一开集 $U$

(1) $f_U:\ F(U)\longrightarrow G(U)$ 是一一的, 当且仅当 $f$ 是 $\mathrm{Sh}(X)$ 中的 monomorphism, 当且仅当 $f_x:\ F_x\longrightarrow G_x$ 是一一的.

(2) $f$ 是 $\mathrm{Sh}(X)$ 中的 epimorphism, 当且仅当 $f_x:\ F_x\longrightarrow G_x$ 是到上的.

以上两命题的证明见 [3].

## §2　Sheaf 上同调

上同调是簇 (variety) 上的一个不变量, 因而可以应用于簇的分类问题的研究. 上同调是一个在理论上和计算上都很有用的工

具，有不同的方法定义上同调.

上同调是定义在 abelian 范畴内的.

**定义 7** 一个范畴 $\mathcal{C}$ 称为一个 abelian 范畴，若满足以下条件：

(1) 对 $\mathcal{C}$ 中每一对对象 $A, B, \mathcal{C}(A,B)$ 是一个可换加群，并且映射的合成 $\mathcal{C}(A,B)\times\mathcal{C}(B,C)\longrightarrow\mathcal{C}(A,C)$ 为双线性 (bilinear) 的；

(2) 具有有限 biproduct (即乘积 (product) 同时又是和 (sum)). 这样特别 0 元既是 initial 对象又是 Ferminal 对象；

(3) 每一个映射具有 kernel 和 cokernel;

(4) 每一个 monomorphism 是一个 kenel, 每一个 epimorphism 是一个 cokernel.

**例 9** 可换群的范畴 Ab 是一个 abelian 范畴.

**例 10** $R$ 是一个环，$R$ 上左模 $R$-mod 与 $R$ 上右模 Mod-$R$ 的范畴均为 abelian 范畴.

**例 11** $X$ 是一个拓扑空间. $X$ 上以可换群为值的 sheaf 构成的范畴 Ab$(X)$ 是一个 abelian 范畴.

**例 12** $(X, Q_x)$ 为一几何空间，$X$ 上的 sheaf $M$ 为 $Q_x$- 模，若对 $X$ 的开集 $U$, $M(U)$ 为 $Q_x$- 模. $Q_x$- 模的范畴 Mod$(X)$ 为一 abelian 范畴.

**定义 8** $\mathcal{C}$ 是一个 abelian 范畴. $\mathcal{C}$ 中的一个 complex$A^{\cdot}$ 是 $\mathcal{C}$ 中的一组对象 $\{A_i, i\in\mathbf{N}\}$, 以及边界映射 $d^i$: $A^i\longrightarrow A^{i+1}$, 并且有 $d^{i+1}\circ d^i=0$, $i\in\mathbf{N}$.($\mathbf{N}=\{0,1,2,\cdots\}$). 两个 complex $A^{\cdot}, B^{\cdot}$ 之间的映射 $f$: $A^{\cdot}\longrightarrow B^{\cdot}$ 是一组映射 $\{f^i: A^i\longrightarrow B^i, i\in\mathbf{N}\}$, $f_i$ 与边界映射 $d^i$ 可换： $f^{i+1}\circ d_A^i=d_B^i\circ f^i$, $i\geqslant 0$. 即以下图形可换

$$\begin{array}{ccc} A^i & \xrightarrow{d_A^i} & A^{i+1} \\ f^i \downarrow & & \downarrow f^{i+1} \\ B^i & \xrightarrow[d_B^i]{} & B^{i+1} \end{array}$$

**定义 9** complex $A^{\cdot}$ 的 $i+h$ 上同调群对象定义为 $h^i(A^{\cdot}) = \frac{\ker d^i}{\operatorname{im} d^{i-1}}$, 这里 $\ker d^i$ 是 $d^i: A^i \longrightarrow A^{i+1}$ 的 kernel, $\operatorname{im} d^{i-1}$ 为 $d^{i-1}: A^{i-1} \longrightarrow A^i$ 的 image. 若 $f: A^{\cdot} \longrightarrow B^{\cdot}$ 是 $A^{\cdot}$ 到 $B^{\cdot}$ 的映射, $f$ 导致一组相应的上同调群之间的同态 $h^i(f): h^i(A^{\cdot}) \longrightarrow h^i(B^{\cdot})$.

**定义 10** $\mathcal{C}$ 是一个 abelian 范畴. $\mathcal{C}$ 中的一个对象 $I$ 称为 injective 若函子 $\mathcal{C}(_, I): \mathcal{C} \longrightarrow \text{Ab}$ 是 exact, 即若 $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ 是 $\mathcal{C}$ 中一个 exact 序列, 则 $0 \longrightarrow \mathcal{C}(C, I) \longrightarrow \mathcal{C}(B, I) \longrightarrow \mathcal{C}(A, I) \longrightarrow 0$ 是范畴 Ab 中的一个 exact 序列.

$A$ 是 $\mathcal{C}$ 中一个对象, $A$ 的一个 injective resolution 是一个 complex $I^{\cdot}$, 其中每一 $I_i$ 是 injective 对象, 并且存在映射 $A \longrightarrow I^0$ 使得

$$0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots \longrightarrow I^n \longrightarrow \cdots$$

是一个 exact 序列.

若 $\mathcal{C}$ 中每一对象具有一个 injective resolution, 我们说范畴 $\mathcal{C}$ 具有足够多的 injective.

$(X, \mathcal{Q}_x)$ 是一个几何空间 (例如 $X$ 是一个仿射簇具有 Zariski 拓扑).$\mathcal{Q}_x$- 模的范畴 $\text{Mod}(X)$ 具有足够多的 injective. 若 $\mathcal{Q}_x$ 为取值整数环 $\mathbf{Z}$ 的常量 sheaf, 那么 $\text{Mod}(X) = \text{Ab}(\text{Sh}(X))$, 所以取值为可换群的 sheaf 的范畴 $\text{Ab}(\text{Sh}(X))$ 具有足够多的 injective.

让 $F$ 是 $\text{Ab}(\text{Sh}(X))$ 的一个对象. $I^{\cdot}$ 为 $F$ 在 $\text{Ab}(\text{Sh}(X))$ 中的一个 injective resolution $0 \longrightarrow F \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots$. 让

这一序列 sheaf 作用在空间 $X$ 上，我们有

$$0 \longrightarrow F(X) \longrightarrow I^0(X) \longrightarrow I^1(X) \longrightarrow I^2(X) \longrightarrow \cdots$$

是范畴 Ab 中的一个 complex, 这是因为 global section 函子 $\mathrm{Ab}(\mathrm{Sh}(X)) \longrightarrow \mathrm{Ab}$, $F \longrightarrow F(X)$ 是一个 left exact 函子.

这样我们定义 sheaf $F$ 的上同调 $H^i(F) = H^i(I^\cdot(X))$, $i \geqslant 0$. 这种方法定义的上同调称为 derived functor cohomology, 这是 Grothendieck 引入的.

**定理 4** $F$ 的任意两个 injective resolution 具有同构的上同调群.

**证明** 见 [2].

**定理 5** $(X, Q_x)$ 是一个几何空间, 用 $\mathrm{Mod}(X)$ 中的 injective resolution 得到的上同调与以上方法得到的上同调是一致的.

**证明** 见 [2].

还有其他方法构造与一个对象相对应的 complex, 用以构造其他类型的上同调群. Serre 引进的 Čeck complex, 提供了直接计算簇上的上同调群的一种方法.

Čeck complex 是这样构造的: $X$ 是一个拓扑空间. 固定 $X$ 上的一个开复盖 $\{U_i\}_{i\in I}$, 良序化 $I$, $F \in \mathrm{Ab}(\mathrm{Sh}(X))$. 定义 $C^n(F) = \prod\limits_{i_0<\cdots<i_n} F(U_{i_0} \cap \cdots \cap U_{i_n})$, $n \geqslant 0$. 由乘积的性质以及 $F$ 是 presheaf, 有 $d_n$: $C^n(F) \longrightarrow C^{n+1}(F)$, $n \geqslant 0$. 相对于这一开复盖 $\{U_i\}_{i\in I}$ 的 Čeck 上同调定义为 $\check{H}^n(F) = h^n(C^\cdot(F))$.

对于拓扑空间 $X$ 以及相应的 sheaf $F$ 加一定条件, 如 $X$ 是仿射簇, $F$ 是一个 coherent sheaf, 或减弱为 $X$ 是可分的 noetherian scheme, $F$ 是 quasi-coherent sheaf, 则有 $\check{H}^n(F) \approx H^n(F)$.

对于一些特殊的拓扑空间以及其上的具有特殊性质的 sheaf, 有关于这些 sheaf 的相应的上同调群的一系列定理.

## § 3 Sheaf 代数几何

代数几何是研究仿射空间和射影空间上多项式方程系统的解的集合的性质和分类的数学,

这里, 首先介绍经典代数几何的主要概念, 然后是以 sheaf 上同调为工具的 Grothendieck 学派的工作, 我们主要讨论仿射空间, 这里给出主要结果, 证明请参阅 [2].

$K$ 是一个代数闭域, $n$ 是任一正整数, 称 $K^n$ 为 $n$ 维仿射空间. $A^n = K[x_1, \cdots, x_n]$ 为 $K$ 上 $n$ 个变量的多项式环. 若 $T$ 为一组多项式, $T \subseteq A^n$, 定义 $Z(T) = \{p \in K^n | f(p) = 0, \forall f \in T\}$, 即 $Z(T)$ 为 $T$ 内多项式的共同零点集, $Z(T)$ 称为 $K^n$ 的一个代数子集.

在 $n$ 维仿射空间 $K^n$ 上定义 Zariski 拓扑如下, $K^n$ 的代数子集 $Z(T)$ 为闭集. 易见这确实构成 $K^n$ 上的一个拓扑.

若 $Y_1 = Z(T_1)$, $Y_2 = Z(T_2)$, 那么 $Y_1 \cup Y_2 = Z(T_1T_2)$; 若 $Y_\lambda = Z(T_\lambda)_{\lambda \in I}$, 那么 $\bigcap\limits_{Y_\lambda \in I} Y_\lambda = Z(\bigcup\limits_{\lambda \in I} T_\lambda)$; $\phi = Z(1)$; $K^n = Z(0)$.

**例 13** 因为 $K$ 是代数闭域, 且 $K[X]$ 的任一理想均为主理想, 所以 $K$ 的闭集 $Z(T) = Z(f) = \{a_1, a_2, \cdots, a_n\}$ 均为 $K$ 的有限子集, $K$ 的开集是有限子集的补集.

下面的命题给出 Zariski 拓扑的一些性质.

**命题 7**

(1) $n$ 维仿射空间 $K^n$ 不可约.

(2) 不可分子集的任一不空开集不可约, 且为稠集.

一个拓扑空间 $X$ 的一个子集 $Y$ 称为不可约的, 若 $Y$ 不能写成两个闭子集 $Y_1, Y_2$ 的并.

这样一维仿射空间 $K$ 上的不可约闭集 $Z(T)$, $T$ 只含有一个不可约多项式 $f$, $Z(T) = Z(f)$.

**定义 11** 一个 $n$ 维仿射代数簇 (affine algebraic variety) 是 $K^n$ 的一个不可约闭集.

仿射代数簇的一个开集称为一个似仿射簇 (quasi-affine variety). 同样可以定义射影空间的射影簇以及似射影簇.

簇 (variety) 指任一仿射簇, 似仿射簇, 射影簇, 或似射影簇.

这样一维仿射代数簇都有形式 $Z(f)$, $f$ 是不可约多项式. $K$ 是代数闭域, $Z(f)$ 为单点集.

**定义 12** $Y$ 是 $K^n$ 的一个子集. $A^n$ 中与 $Y$ 相应的理想 $I(Y)=\{f\in A^n|f(p)=0,\forall\, p\in Y\}$.
$Y$ 的仿射座标环定义为 $A(Y)=\frac{A^n}{I(Y)}$.

**命题 8**

(1) $K^n$ 的代数子集一一对应于 $A^n$ 的 radical 理想 ($B$ 是 radical 理想, 若 $B$ 的 radical $\sqrt{B}=B$),

$$Y\longmapsto I(Y),\quad B\longmapsto Z(B)$$

特别, $Y$ 是仿射代数簇当且仅当 $I(Y)$ 是素理想.

(2) 仿射代数簇 $Y$ 一一对应于为整环的有限生成的 $K$- 代数 $\frac{A^n}{I(Y)}$.

**定义 13**

(1) $X$ 是一个拓扑空间, $X$ 的维数定义为 $X$ 中不可约闭集链的长度的上极限.

(2) $A$ 是一个可换环, $A$ 的高度定义为 $A$ 中素理想链长度的上极限.

**命题 9** 仿射簇的维数等于它的座标环的高度.

以下我们要定义簇之间的映射, 因而 $K$ 上的簇以及它们之间的映射构成一个范畴 Var$(K)$. 而维数是簇的一个不变量.

一组多项式 $T$ 的共同零点这一代数概念又是仿射空间 $K^n$ 的一个几何实体 $Z(T)$. 这一几何实体对应于交换代数中的理想

$I(Z(T))$ 或 $K$- 代数 $\frac{A^n}{I(Z(T))}$. 交替使用 $K^n$ 上 Zariski 拓扑的性质，$A^n$ 中交换代数的性质，我们可以得到相应的有关簇的知识，如以上命题中仿射簇的维数及其座标环的高度的一一对应关系.

人们还揉进函数，分析的有关知识与交换代数一起用来研究簇的分类问题.

**定义 14** $Y$ 是 $K^n$ 的一个簇，$Y$ 上 $K$ 值函数 $f: Y \longrightarrow K$ 称为在 $p \in Y$ 点正则 (regular)，若存在 $p$ 点的一个开邻域 $U \subseteq Y$，多项式 $g, h \in A^n = K[x_1, x_2, \cdots, x_n]$，使得在 $U$ 中 $f = \frac{g}{h}$，$h \neq 0$. 若 $f$ 在 $Y$ 的任一点 $p$ 正则，我们说 $f$ 是一个正则函数.

**命题 10** $f: Y \longrightarrow K$ 为一正则函数. 若 $K$ 具有 Zariski 拓扑，那么 $f$ 是一连续函数.

簇之间的映射定义如下：

**定义 15** $X, Y$ 是两个簇. $X$ 到 $Y$ 的一个映射 $\phi: X \longrightarrow Y$ 是一个连续映射，并且对 $Y$ 的任意开集 $V \subseteq Y$，$V$ 上任一正则函数 $f: V \longrightarrow K$，$f \circ \phi: \phi^{-1}(V) \longrightarrow K$ 仍是一正则函数.

这样 $K$ 上的簇与它们之间的映射构成一个范畴 Var$(K)$.

下面定义与簇有关的几个函数环. $Y$ 是一个簇.

**定义 16**

(1) $Q(Y)$ 由 $Y$ 上所有正则函数构成.

(2) $p \in Y$，$Q_p$ 由元素 $(U, f)$ 组成. 这里 $U \subseteq Y$ 为 $p$ 的一个开邻域，$f: U \longrightarrow K$ 为 $U$ 上一个正则函数. $(U, f) = (V, g)$ 当且仅当 $f|_{U \cap V} = g|_{U \cap V}$.

(3) $Y$ 的有理函数域 $K(Y)$，由元素 $(U, f)$ 构成. $U$ 是 $Y$ 的一个开集，$f$ 为 $U$ 上的正则函数. $(U, f) = (V, g)$ 当且仅当 $f|_{U \cap V} = g|_{U \cap V}$.

注　首先可以检验 (2),(3) 中定义的二元关系确是等价关系.

$Q_p$ 是一个局部环 (local ring)，$Q_p$ 具有极大理想. $I = \{(U, f) \mid f(p) = 0\}$. 因为 $Y$ 是不可约的，所以 $Y$ 上两个开集的交 $U \cap V \neq$

$\phi$, 所以可以在 $K(Y)$ 上定义加法与乘法. 若 $(U,f)$, $f \neq 0$, 那么 $V = U-(U\cap Z(f))$ 仍为开集, 且在 $V$ 上 $f \neq 0$. 即 $(V, \dfrac{1}{f})$ 是 $(U,f)$ 的逆. 这样 $K(Y)$ 是一个域.

我们有 $Q(Y) \hookrightarrow Q_p \hookrightarrow K(Y)$.

仿射簇 $Y$ 的仿射座标环 $A(Y)$ 与 $Q(Y)$, $Q_p$, $K(Y)$ 有以下关系.

**定理 6** $Y$ 是一个仿射簇.

(1) $Q(Y) \approx A(Y)$. 进一步, 若 $X$ 是另一仿射簇, $X$ 同构于 $Y$ 当且仅当作为 $K$- 代数 $A(X)$ 同构于 $A(Y)$.

(2) $m_p = \{f \in A(Y) | f(p) = 0\}$.$m_p$ 为 $A(Y)$ 的极大理想. $Y$ 中的点一一对应于 $A(Y)$ 的极大理想, 对应关系 $p \longleftrightarrow m_p$.

(3) $Q_p \approx A(Y)_{m_p}$.

(4) $K(Y)$ 同构于 $A(Y)$ 的商域.

代数几何是研究族的分类问题.

由以上定理我们看到仿射簇的同构对应于作为整环的有限生成的 $K$- 代数.

一下子做同构意义下的分类不容易, 人们又引进了簇之间的 birational 等价关系, 这里我们不具体介绍 birational 等价关系的定义, 而给出有关结果.

**定理 7** $X, Y$ 为两个簇, 以下条件等价:

(1) $X$ 和 $Y$ birational 等价.

(2) 存在 $X$ 的开集 $U$,$Y$ 的开集 $V$,$U$ 同构于 $V$.

(3) $K(X)$ 和 $K(Y)$ 作为 $K$- 代数同构.

曲线 (一维), 曲面 (二维) 的 birational 分类问题基本得到了解决.

以 Grothendieck 为代表的法国学派推广了簇的概念, 引进 scheme, 以及 sheaf 的上同调 (cohomology) 为簇的另一不变量, 研究簇

的分类问题，进一步推动了代数几何的发展.

我们知道一个仿射簇对应于一个为整环的有限生成的 $K$- 代数，Grothendieck 认为不必局限于这样范围狭窄的一类环，他取任一可换环 $A$. 定义一个与 $A$ 相应的拓扑空间 $\operatorname{spec} A$.

**定义 17** $A$ 是一个可换环，$\operatorname{spec} A$ 由 $A$ 的素理想构成，若 $I$ 为 $A$ 的一个理想，让 $V(I) = \{P \in \operatorname{spec} A | I \subseteq P\}$.

若 $I,J$ 是 $A$ 的理想，$V(I) \cup U(J) = V(IJ)$; $\{I_i\}$ 为 $A$ 的一组理想，$\bigcap_i V(I_i) = V(\sum_i I_i)$; $V(\{0\}) = A$, $\{0\}$ 是 $A$ 的零理想; $V(A) = \phi$.

这样 $\{V(I)\}$ 构成 $\operatorname{spec} A$ 上一个拓扑的闭集.

**例 14** $K$ 是一个域，$\operatorname{spec} K = \{0\}$.

**例 15** $K$ 是一个代数闭域，$\operatorname{spec} K[x] = K \cup \{\xi\}$, 这里 $\xi$ 是所谓的 generic point, 对应于零理想. $\operatorname{spec} K[x]$ 称为仿射线 (affine line). $\xi$ 的闭包 $\overline{\xi} = \operatorname{spec} K[x]$.

**例 16** $f \in K[x,y]$ 是一不可约多项式. $I(f)$ 是 $K[x,y]$ 的素理想. 这样 $\operatorname{spec} K[x,y]$ 的闭点集正是 $K^2$, 而每一个不可约多项式 $f$ 对应于 $\operatorname{spec} K[x,y]$ 中的一个点 $\eta_f$, $\eta_f$ 的闭包 $\overline{\eta}_f = \{(k_1,k_2)|f(k_1,k_2) = 0\}$, 即曲线 $f(x,y) = 0$. 零理想对应于 $\overline{\xi}$, $\overline{\xi} = \operatorname{spec} K[x,y]$.

若 $f: A \longrightarrow B$ 是一个环同态，定义 $\operatorname{spec} f: \operatorname{spec} B \longrightarrow \operatorname{spec} A$ 为 $\operatorname{spec} f(P) = f^{-1}(P)$. $(\operatorname{spec} A)^{-1}(V(I)) = V(f^{-1}(I))$. $\operatorname{spec} f$ 是一连续映射.

这样，spec 给出从 $\mathrm{Ring}^{op}$ 到 Top 的一个函子，spec: $\mathrm{Ring}^{op} \longrightarrow$ Top. 这是一个联系代数范畴与几何范畴的函子.

下面定义拓扑空间 $\operatorname{spec} A$ 上的一个取值为可换环的 sheaf $Q_{\operatorname{spec} A}$.

对 $A$ 的一个素理想 $P$, $A_P$ 为 $A$ 在 $P$ 点的局部化 (localization of $A$ at $P$), 对 $\operatorname{spec} A$ 的一个开集 $U$, $Q_{\operatorname{spec} A}(U) = \{s : U \longrightarrow$

$\coprod_{P\in U} | s(P) \in A_P$ 并且存在 $P$ 的一个开邻域 $V \subseteq U$, $a, f \in A$, 对 $V$ 中任一点 $R$ 有 $f \notin R$, 且 $s(R) = \frac{a}{f}\}$.

比较 $s$ 与正则 (regular) 函数.

不难检验 (1) $Q_{\mathrm{spec}\,A}(U)$ 是一个有单位元的可换环; (2) $Q_{\mathrm{spec}\,A}$ 是一个 presheaf;(3) 进而 $Q_{\mathrm{spec}\,A}$ 是一个 sheaf.

**定义 18** $A$ 是一个环, $(\mathrm{spec}\,A, Q_{\mathrm{spec}\,A})$ 称为 $A$ 的 spectrum. $Q_{\mathrm{spec}\,A}$ 称为 $A$ 的结构 sheaf(structure sheaf).

$f \in A$, 让 $D(f) = \mathrm{spec}\,A - V((f))$ 为 $V((f))$ 在 $\mathrm{spec}\,A$ 中的补集.

**命题 11** $A$ 是一个环, $(\mathrm{spec}\,A, Q_{\mathrm{spec}\,A})$ 为 $A$ 的 spectrum.

(1) $Q_{\mathrm{spec}\,A}(D(f)) \approx A_f$, $A_f = A[\frac{1}{f}]$.

(2) 对任一 $P \in \mathrm{spec}\,A$, sheaf $Q_{\mathrm{spec}\,A}$ 在 $P$ 点的 stalk$(Q_{\mathrm{spec}\,A})_P \approx A_P$.

(3) 特别 $Q_{\mathrm{spec}\,A}(\mathrm{spec}\,A) = A$.

若 $g: A \to B$ 是一个环同态, 我们知道 $\mathrm{spec}\,g : \mathrm{spec}\,B \to \mathrm{spec}\,A$ 为一连续映射, 并且 $g_P: A_{g^{-1}(P)} \to B_P$ 是一个局部同态. 定义 $(g^{-1}(Q_{\mathrm{spec}\,B}))(U) = Q_{\mathrm{spec}\,B}((\mathrm{spec}\,g_{-1})(U))$. 这样 $g^{-1}(Q_{\mathrm{spec}\,B})$ 是 $\mathrm{spec}\,A$ 上的一个 *sheaf*. $g^{\#}: Q_{\mathrm{spec}\,A} \to g^{-1}(Q_{\mathrm{spec}\,B})$ 定义如下: 让 $U$ 是 $\mathrm{spec}\,A$ 的一个开集, 若 $s \in Q_{\mathrm{spec}\,A}(U)$, 那么以下映射的合成给出 $Q_{\mathrm{spec}\,B}((\mathrm{spec}\,g)^{-1}(U))$ 的一个元素:

$$(\mathrm{spec}\,g)^{-1}(U) \xrightarrow{g} U \xrightarrow{s} \coprod_{g^{-1}(P)\in U} A_{g^{-1}(P)} \xrightarrow{\coprod_{g^{-1}(P)\in U} g_P} \coprod_{g^{-1}(P)\in U} B_P.$$

这样环同态 $g: A \longrightarrow B$ 导致 $(\mathrm{spec}\,B, Q_{\mathrm{spec}\,B})$ 到 $(\mathrm{spec}\,A, Q_{\mathrm{spec}\,A})$ 的一个映射 $(\mathrm{spec}\,g, g^{\#})$.

推广 $A$ 的 spectrum$(\mathrm{spec}\,A, Q_{\mathrm{spec}\,A})$ 的想法, 有以下关于几何

空间的定义.

**定义 19** $(X,Q_X)$ 称为几何空间. 这里 $X$ 是一个拓扑空间, $Q_X$ 是 $X$ 上以可换环为值的 sheaf, 并且对 $X$ 的任一点 $P$, $\mathrm{stalk}(Q_X)_P$ 是一局部环.

若 $(Y,Q_Y)$ 是另一几何空间, $(X,Q_X)$ 到 $(Y,Q_Y)$ 的一个映射 $(f,f^*)$: $(X,Q_X)\longrightarrow(Y,Q_Y)$ 由两部分组成, $f: X\longrightarrow Y$ 为一连续映射, $f^*: Q_Y\longrightarrow f^{-1}Q_X$. $f^*$ 具有性质, $f_x^*$: $Q_{f(x)}\longrightarrow Q_x$ 是局部的, 即 $f_x(m_{f(x)})\subseteq m_x$. 这里 $m_x$ 是含 $x$ 的极大理想.

例如, 让 $Q_X,Q_Y$ 分别为 $X$ 和 $Y$ 上的连续复值函数. $f$ 是 $X$ 到 $Y$ 的一个连续映射, $f^*Q_Y(U)=Q_X(f^{-1}(U))$, 若 $g\in Q_Y(U)$, $g: U\longrightarrow \mathbf{C}$, 那么 $f^*(g)=g\circ f$: $f^{-1}(U)\longrightarrow U\longrightarrow\mathbf{C}$, 并且 $f_x^*$: $Q_{f(x)}\longrightarrow Q_x$ 在相应的 stalk 上是局部的环同态. $(f,f^*)$ 是 $(X,Q_X)$ 到 $(Y,Q_Y)$ 的一个映射.

记几何空间的范畴为 GE, 这正是代数几何的活动范畴.

这样 $(\mathrm{spec},Q_{\mathrm{spec}})$ 成为从可换环的范畴到几何空间范畴的一个反变函子. 我们简记 $(\mathrm{spec},Q_{\mathrm{spec}})$ 为 spec. 实际上代数几何中的可换环都是一个代数闭域 $K$ 上的代数. 所以取 $K$- 代数的范畴 $K$-alg, 它是可换环范畴的一个子范畴. 并要求 $Q_X$ 为取值为 $K$- 代数的 sheaf. 几何空间的范畴仍记为 GE.

**定理 8** 函子 spec: $K\text{-alg}^{\mathrm{op}}\longrightarrow \mathrm{GE}$ 是满的和忠实的. 这样可以将范畴 $K\text{-alg}^{\mathrm{op}}$ 看为几何空间范畴 GE 的一个子范畴.

$(X,Q_X)$ 是一个几何空间. 那么 $T((X,Q_X))=Q_X(X)$ 是一个 $K$- 代数. 若 $(f,f^*)$: $(X,Q_X)\longrightarrow(Y,Q_Y)$, 则 $T((f,f^*))=f_Y^*$: $Q_Y(Y)\longrightarrow f^{-1}Q_X(Y)=Q_X(f^{-1}(Y))=Q_X(X)$ 是一个 $K$- 代数同态. 这样 $T$: $GE\longrightarrow K\text{-alg}^{op}$ 是一个函子.

**定理 9** $T$ 是 spec 的 left adjoint.

**定义 20** 一个几何空间 $(X,Q_X)$ 是一个仿射 scheme, 若存在 $K$- 代数 $A$, $(X,Q_X)$ 同构于 $(\mathrm{spec}\,A,Q_{\mathrm{spec}\,A})$. 一个几何空

间 $(X, Q_X)$ 称为一个 scheme, 若有 $X$ 的一个开复盖 $\{U_i\}$ 并且 $(U_i, Q_x|_{U_i})$ 是一个仿射 scheme.

这样仿射 scheme 与 $K$- 代数大致是一回事，而 scheme 局部与 $K$- 代数是一回事.

$V$ 是 $K$ 上一个仿射簇，$Q_V$ 是 $V$ 上正则函数的 sheaf. $Q_V(V)$ 同构于 $V$ 的仿射座标环 $A(V)$. 那么 $(V, Q_V)$ 与 $(\operatorname{spec} A(V), Q_{\operatorname{spec} A(V)})$ 有什么关系呢？

首先我们知道，$V$ 的不可约闭集一一对应于 $A(V)$ 中的素理想. 对拓扑空间 $V$ 定义一个新的拓扑空间 $t(V)$, $t(V)$ 由 $V$ 中不可约闭子集构成. $t(V)$ 的闭集由 $t(Y)$ 的子集组成，这里 $Y$ 是 $V$ 中的闭集 (检验这确实构成 $t(V)$ 的闭集).

于是我们有 $\operatorname{spec} A(V)$ 同胚于 $t(V)$, 并且 $\alpha : V \to t(V)$, $\alpha(x) = \overline{\{x\}}$, $\alpha$ 使 $V$ 同胚于它的像. 不难证明 $Q_{\operatorname{spec} A(V)} \approx \alpha^{-1} Q_V$. 这样 $(t(V), \alpha^{-1} Q_V)$ 同构于 $(\operatorname{spec} A(V), Q_{\operatorname{spec} A(V)})$.

$(X, Q_X)$ 是一个 scheme, $\operatorname{Mod}(X)$ 是 $Q_X$- 模的范畴. 不难证明 $\operatorname{Mod}(X) \approx \operatorname{Ab}(\operatorname{Sh}(X))$. 定义上同调函子 $H^i(X, \cdot)$ 为 $T(X, \cdot)$ 的 right derived 函子. $\mathcal{F}$ 是一个 sheaf, $H^i(X, \mathcal{F})$ 为 $\mathcal{F}$ 的上同调群. 同样可以定义 Cěck 上同调.

空间 $X$ 的不同性质，如 noetherian, sheaf 的不同性质，如 flasque, coherent, quasi-coherent 等，与上同调群的不同性质有相关的对应.

用 sheaf 的上同调为工具可以得到一系列所谓 vanishing 定理.

Grothendieck vanishing 定理. $X$ 是一个 $n$ 维 noetherian 拓扑空间. 那么对于 $i > n$, $\mathcal{F} \in \operatorname{Ab}(\operatorname{Sh}(X))$ 有 $H^i(X, \mathcal{F}) = 0$.

用 scheme 的上同调来研究曲线的分类，曲面的分类有一系列的定理.

# 参考文献

1 Demazure M, Gabrial P. Introduction to Algebraic Geometry and Algebraic Groups. Amsterdam: North–Holland Publ. Co., 1980

2 Hartshorne R. Algebraic Geometry. Heidelberg: Springer–Verlag, 1977

3 Tennison B R. Sheaf Theory. Cambridge: Cambridge Univ. Press, 1975

# 第 20 章

## 数学基础与范畴论

F. W. Lawvere 教授一再强调：范畴论不只是一个数学学科，而更是方法论. 它为我们提供了一种从全局认识问题、分析问题，从中找出一般的、抽象的、有决定意义的关系的方法.

自上世纪末至今，集合论成为传统数学基础研究的中心. 数学基础的研究逐渐形成了一个独立的数学分支，与其他数学学科几乎没有联系，更不要提像物理学这样的其他自然科学学科. 以至很多数学家对数学基础的研究不屑一顾，你建筑你的数学基础，我搞我的具体研究.

Lawvere 教授对什么是数学基础与传统的观念有很不同的看法. 他认为，真正的基础必须为数学服务，必须为发现和应用几何、分析、统计、物理、计算机等学科中的正确概念提供指导 (guide)，而且为发现恰如其分的猜想、论断，以及证明这些猜想、论断提供指导.

Lawvere 在 1989 年说过一段对数学基础的研究很有指导意义的话：“Mathematics is the science of space forms and quantitative relationships; thus the core of Mathematics is geometry and analysis and their mutual transformation. Logic is the development of

thinking in its necessity. Hence the investigation of the Logic of Mathematics means the detailed study of the laws of the development of our thinking about geometry and analysis, with the sole purpose of clarifying and simplifying the learning, use, and development of mathematics by all those who need it. In the main, each of abstract algebra, general topology, mathematical logic, set theory, is the result of certain definite discoveries in the Logic of Mathematics as well as of definite discoveries in Mathematics itself. Even though category theory sums up and includes abstract algebra, general topology, mathematical logic, and set theory, it also runs the risk of becoming a separated hranch if the purpose stated above is lost sight of. Thus I have devoted a good part of my "Advanced Course on Category Theory"to attempting to learn, to clarify for the students, and to assist them in simplifying significant parts of Analysis. And while one major effect of my contributions to topos theory has been to enable the latter to be applied to clarifying model theory, set theory, and proof theory, I constantly emphasize that the actual intended purpose of these contributions is to permit the clarification of geometry, analysis and physics,"

注意， Lawvere 在这段话里的 logic(逻辑) 一词是广义的，不是指数理逻辑.

他强调说：

"Why must we study the foundations of Mathematics? Why we must study the history of Mathematics?

According to my interpretation we must study the history of Mathematics in order to arrive to the foundations of Mathematics, in order to discover the laws of the development of scientific thought, both objective and subjective. Why must we know these

laws? About all to arrive at a position from which we can teach these laws. And why teach them? In order to assist the Learning, Development and Utilization of Mathematics itself, that is the science of space and quantity."

Lawvere 以范畴论为工具进行数学基础的研究. 范畴论被很多数学家认为是 "abstract nonsense", 这是有一定原因的: 因为有一批为数不少的搞范畴论的数学家, 比如法国以及澳大利亚的一部分数学家, 正象 Lawvere 教授警告的那样, 他们把范畴论搞成了一个专门的玄而又玄的数学分支.

但是主流的搞范畴论的数学家并不是这样, 他们学习研究范畴论是有明确目的的: 用范畴论做工具去分析研究各数学学科之间的不同与相同性, 建立数学是一个整体的观念, 认识到不同数学分支与这个整体的联系, 以及它们之间的联系与转化. 从而提出新概念, 发现新关系, 新理论, 进而推动数学的学习, 研究, 发展, 应用与教学. 而不只是 justify 历史上著名数学家提出的问题与猜想.

这部份以 Lawvere 教授为代表的数学家的新观点, 同一切新生事物一样, 开始时是不受重视的. 但是随着数学和其他科学的发展, 随着他们工作的开展, 人们渐渐认识到他们工作的重要性.

1990 年 6 月份在英国剑桥大学举办了一个专题讨论会 (workshop), 请 Lawvere 教授主讲 "Category Theory and the foundations of Mathematics".

这里将简要介绍 Lawvere 教授对数学基础的研究工作.

1. Mengen 和 Kardinalen (variable sets and abstract sets);

2. 空间的范畴;

3. 空间和量;

4. Intensive and extensive quantities

## § 1　Mengen 和 Kardinalen
## (variable sets and abstract sets)

Lawvere 教授指出，Cantor 原意的 Mengen 和 Kardinalen 与现代集合论意义下的集合 (sets) 和基数 (cardinals) 是很不一样的.

Cantor 开始于研究数论，之后是傅立叶级数 (Fourier series). 他特别对有关的，能使某些傅立叶级数收敛的 Mengen 感兴趣. 他感到必须进一步一般地学习研究这些 Mengen. 一个 Menge 是由一些点组成，但这些点不是孤立的没有联系的. 这些点是有某种内聚性的 (Cohesion). 如果我们只考虑一个 Menge 的点，忽略掉它的内聚性，那么我们得到这个 Menge 所对应的 Kardinale.

若两个 Mengen 所对应的 Kardinalen 间存在一个一一到上的映射 (即一个可逆映射), 则说这两个 Mengen 等势 (equi-cardianlity). 这样等势的概念是在某种同构 (isomorphism) 意义下的. Cantor 称为 Maechtigkeit.

有意思的是，Cantor 的 Maechtigkeit 是引用瑞士几何学家 Jakob Steiner 的. 1850 年，Steiner 在研究圆锥曲线 (conic sections) 时，用到 Maechtigkeit, 去说明椭圆和抛物线以及抛物线和双曲线 potency 的不等价. 当然，Cantor 用 Maechtigkeit 于一种更抽象的意义下. Cantor 说，他的 Maechtigkeit 的概念不同，但是相象于 Steiner 的 Maechtigkeit. 范畴论的萌芽已在这里出现.

Cantor 的 Kardinalen 是由抽象集合 (abstract sets) 以及抽象集合之间的任意映射构成的范畴 $S$. $S$ 可以由一组公理来严格刻画. 参看 [2]. 直观上说，一个抽象集合 (即一个 Kardinale)$K$ 是由一些点 (points) 组成、除了两个点可能相等或不等之外，没有其他结构. 两个抽象集合 $K, K'$ 等价，当且仅当存在从 $K$ 到 $K'$ 的一个可逆映射.

Mengen 是从几何与分析中得到的概念. 具有某种内聚性的 Mengen 及它们之间保持这种内聚性的映射构成一个范畴. 例如拓扑空间以及连续映射构成的范畴 Top; 另外如 Burnlogical spaces 的范畴和 combinatorial spaces 的范畴.

这样一个抽象集合 (Kardinale, cardinal number) 是一个特殊的 Menge, 因为离散是一种特殊的内聚性.

我们不仅应该研究具有特殊内聚性的空间的特殊性质, 而且应该研究一般具有内聚性变化性空间的一般性质. Lawvere 把一个具有内聚性的空间称为 variable set, 我们用 $\mathfrak{M}$ 表示具有某种内聚性的 variable sets 与保持这种内聚性的态射构成的范畴.

首先, 什么是 $\mathfrak{M}$- 空间 (即 $\mathfrak{M}$ 中对象 (object))$M$ 的点? 因为 $\mathfrak{M}$ 有 terminal object 1, 如在 Top 中, terminal object 是一个点的拓扑空间. $\mathfrak{M}$- 空间 $M$ 的点定义为从 1 到 $M$ 的态射. 这样 $M$ 的点 $=\mathfrak{M}(1,M)$. 一个拓扑空间的点正是通常意义下的点.

对任一 $\mathfrak{M}$- 空间 $M$, 我们可以结合它的 Kardinale, 即由 $M$ 的点组成的抽象集合 $\text{pts}(M)=\mathfrak{M}(1,M)$. 两个 $\mathfrak{M}$- 空间 $M,M'$ 具有相同的 cardinality 或等势, 当且仅当它们所对应的抽象集合 $\text{pts}(M)$ 与 $\text{pts}(M')$ 在 $S$ 中等价. 这样, cardinality 是 $\mathfrak{M}$- 空间的一个不变量.

从一个抽象集合 (Kardinale, cardinal number) $K$ 可以构造一个 $\mathfrak{M}$- 空间 $\text{dis}(K)$. 例如 $\mathfrak{M}=$Top, 那么 $\text{dis}(K)$ 是由 $K$ 生成的离散 (discrete) 拓扑空间.

pts 是从 $\mathfrak{M}$ 到 $S$ 的函子, 把一个 $\mathfrak{M}$- 空间 $M$ 送到它所对应的点的抽象集合 $\text{pts}(M)$; dis 是 $S$ 到 $\mathfrak{M}$ 的函子. dis 是 pts 的 left adjoint, $\text{dis}\dashv\text{pts}$, 即对 $\mathfrak{M}$- 空间 $M$, 抽象集合 $K$, 有如下自然一一对应关系:

$$\begin{array}{c|ll} \downarrow\uparrow & \mathrm{dis}(K) \longrightarrow M & \text{在 } \mathfrak{M} \text{ 中} \\ \hline & K \longrightarrow \mathrm{pts}(M) & \text{在 } \mathcal{S} \text{ 中} \end{array}$$

这样从 $\mathfrak{M}$- 空间 $\mathrm{dis}(K)$ 到 $M$ 的连续映射 ($\mathfrak{M}$ 中的态射), 一一对应于从抽象集合 $K$ 到 $\mathrm{pts}(M)$ 之间的任意映射.

若取 $K=\mathrm{pts}(M')$, 则我们有 $\mathfrak{M}$ 中的态射

$$\frac{\mathrm{dis}(\mathrm{pts}(M')) \longrightarrow M}{\mathrm{pts}(M') \longrightarrow \mathrm{pts}(M)}$$

对应于 $\mathcal{S}$ 中映射

即 $\mathrm{dis}(\mathrm{pts}(M'))$ 到 $M$ 的连续映射是任意的 (一一对应于 $\mathrm{pts}(M')$ 到 $\mathrm{pts}(M)$ 的任意映射). 这是因为 $\mathrm{dis}(\mathrm{pts}(M'))$ 的每一个点都是开集.

我们取 $K=\mathrm{pts}(M)$, 则对应于恒等映射

$$\frac{1_{\mathrm{pts}(M)}: \mathrm{pts}(M) \longrightarrow \mathrm{pts}(M)}{\mathrm{dis}(\mathrm{pts}(M)) \longrightarrow M}$$

的

是连续映射. 这是 $M$ 的点到 $M$ 的嵌入.

函子 $\mathrm{pts}: \mathfrak{M} \longrightarrow \mathcal{S}$ 还有一个 right adjoint codiscrete 或 chaotic. 若 $\mathfrak{M}=\mathrm{Top}$, $\mathrm{chao}(K)$ 是 $K$ 生成的非离散空间. 我们没有任何关于 $\mathrm{chao}(K)$ 中具体的内聚性的信息, 因为 $\mathrm{chao}(K)$ 的开集只有它本身和空集, 所以称为 chaotic.

$$\text{discrete} \left(\begin{array}{c} \mathfrak{M} \\ \uparrow \ \big\downarrow \mathrm{pts} \ \uparrow \\ \mathcal{S} \end{array}\right) \text{chaotic} \qquad \begin{array}{c|ll} \downarrow\uparrow & \mathrm{dis}(K) \longrightarrow M & \text{在 } \mathfrak{M} \text{ 中} \\ \hline & K \longrightarrow \mathrm{pts}(M) & \text{在 } \mathcal{S} \text{ 中} \\ & M \longrightarrow \mathrm{chao(K)} & \text{在 } \mathfrak{M} \text{ 中} \\ \hline \downarrow\uparrow & \mathrm{pts}(M) \longrightarrow K & \text{在 } \mathcal{S} \text{ 中} \end{array}$$

从 $M$ 到 chao($K$) 的态射是任意的 (一一对应于 pts($M$) 到 $K$ 的任意映射). 而从 $M$ 到 dis($K$) 的态射却绝对不是任意的. 例如在 Top 中, 若 $M$ 是连通的 (connected), 则不存在 $M$ 到 dis(2) 的非常连续映射 (non-constant continuous map), 这里 2 是两个元素的抽象集合. Lawvere 建议用 "不存在 $M$ 到 dis(2) 的非常态射" 作为 $\mathfrak{M}$- 空间 $M$ 连通的条件. 在任意具有 terminal object 1 的范畴中, $X$ 到 $Y$ 的态射 $f: X \longrightarrow Y$ 是常态射 (constant morphism), 如果存在从 1 到 $Y$ 的一个态射, 使得以下三角形可换:

$$\begin{array}{ccc} X & \xrightarrow{t} & Y \\ \downarrow & \nearrow & \\ 1 & & \end{array}$$

一般来说, 一个离散空间完全缺乏内聚性. 它的每一个点都是孤立的, 从而运动在离散空间内是不可能的, 因为没有从连通空间到它的一个态射能经过两个不同的点. (通常 $M$ 内的运动以时间为参数, 即是一个从时间到 $M$ 的态射, 而时间构成一个连通空间.) 而非离散空间又是内聚性过剩. 非离散空间中的任一点可以不经任何努力随便搬到另一点: 因为从任一 $\mathfrak{M}$- 空间 $M$ 到 chao($K$) 的态射就是抽象集合 pts($M$) 到 $K$ 的任意映射.

有很特殊的 Mengen 的范畴 (combinatorial 特性的)$\mathfrak{M}$ 如 simplicial complexes. 在某种意义上说由 chaotic 对象生成的. 一个 $\mathfrak{M}$- 空间 $M$, 完全决定于一系列态射

$$\text{chao}(K) \longrightarrow M, \text{对每一个有限 } K.$$

离散与非离散空两唯一决定于它们的基数 (cardinality). 我们有 ptsodis$\approx 1_S$ 和 ptsochao$\approx 1_S$. 这里 $1_S$ 是 $S$ 到 $S$ 的恒等函子. 这样对任一抽象集合 $K$,

$$\text{pts}(\text{dis}(K)) \approx K \quad \text{和} \quad \text{pts}(\text{chao}(K)) \approx K$$

或对任一 $\mathfrak{M}$- 空间 $M$、

$$\text{pts}(\text{dis}(\text{pts}(M)) \approx \text{pts}(M) \text{ 和 } \text{pts}(\text{chao}(\text{pts}(M))) \approx \text{pts}(M).$$

虽然通常 dis(pts($M$)) 与 $M$, chao(pts($M$)) 与 $M$ 是不同构的.

这样, $\mathfrak{M}$ 含有两个与 $S$ 等价的子范畴, 一个由离散空间组成, 一个由非离散空间组成.

1985 年秋天, Lawvere 教授给本科生和研究生开了一门代数集合论的课. 第一讲, 他没有用他的讲义上提出的公理来严格刻画抽象集合的范畴 $S$, 却提出了这样较为直观的理解. 他说到一个抽象集合是由一些点组成的. 除了两点可以相等或不等以外别无其他结构、性质. 一个 5 个点的抽象集合可以用 来表示, 当然袋子是没有形状的. 当时著名的逻辑学家 John Myhill 教授也在场. 他听到这儿说: "等一下, 我以前在什么地方好像听到过这样的描述." 想了一会儿, 他说是 Cantor. 第二天他告诉 Lawvere, 在 Cantor 著作的第 283 页, Cantor 用了同样的描述于 Kardinalen. Lawvere 在这之前并没有阅读 Cantor 的著作, 但他提出的 abstract sets 的概念与 Cantor 的 Kardinalen 却是基本一致的.

这么多年来为什么没有人认真研究一下 Cantor 的著作呢? Lawvere 教授指出, 一些著名数学家的著作选集的编辑的观点对以后的人们学习这些数学家的著作有很大影响. 有时这些编辑们作出错误的评价, 以致给后人以错误的引导. Cantor 选集的编辑 Zermelo 说, Cantor 的这部分论述 (关于 Kardinalen) 是自相矛盾的, 我们应该直接过渡到 cardinal 的算术, 即现代意义的 cardinal. 他说, 没有任何性质怎么能够区别不同与相同呢? 这是真正的矛盾.

现在用 adjoint functors 可以帮助我们很好地理解这一使 Zermelo 感到困惑的问题.

通过由一个 Kardinale $K$ 生成的离散空间与 $\mathfrak{M}$- 空间的联系,

$K$ 的点是完全可以区别的. 而另一方面通过相应的 $K$ 生成的非离散空间与 $\mathfrak{M}$- 空间的联系，它的点又是完全不能区别的.

Lawvere 说： "The 'inconsistency' of diversity versus indistinguishability, of having a definite number of points, but of these points being indistinguishable by any property, seemed to Zermelo so antagonostic a contradiction that nothing coherent could be done. But the explicit use of adjoint functors between categories on this configuration lays every thing out so that the productive nature of this contradiction can become clear to everyone".

一个面一个空间 $M$ 的 Kardinale pts($M$) 具有一定数量的点，即不同的点. 因为 dis(pts($M$)) $\longrightarrow M$ 是一个 monomorphism (简单说来是一个单射. 虽然一般 monomorphism 和单射是不同的概念). 所以这些点像它们在 $M$ 中一样仍是不同的. 而另一方面，对于 chao(pts($M$)) 没有任何性质可以区别它的点，因为 chao(pts($M$)) 到任一 discrete space 的态射都是常态射 (一个空间的一个性质，可以划分这个空间的点为一些等价类. 这相当于从这个空间到某一离散空间的态射). 更进一步通过从连通空间到 chao(pts($M$)) 的某个态射，可以把一个点搬到任意另一个点.

## §2 空间的范畴

一个 topos 具有逻辑的与几何的特性.

从几何意义上说，topos 有两种. 作为一个广义的空间 (a generalized space), 例如一个拓扑空间 $X$ 上的 sheaf 构成的范畴 Sh($X$); 与作为空间的范畴 (topos of spaces), 例如 Johnston topos(拓扑空间), Grothendieck 的 analytic 空间的范畴，组合 (combinatorial) 空间的范畴等.

Lawvere 教授希望能有一组公理刻画这种作为空间的范畴的

topos. 因为这对于研究空间与数量的一般关系，以及形式化物理学中很多问题是必要的.

他说："There are certain properties which a topos of spaces often has; a wise selection of these should serve as an axiomatic definition of the subject. While we have not achieved that goal yet, we list some important properties and show that these properties can not be true for a 'generalized space' of the localic or groupoid kind".

他提出三条. 让 $\mathcal{E}$ 是一个 $\mathcal{S}$ 上的 topos ($\mathcal{E}$ 是 $\mathcal{S}$ 上的一个 topos, 即存在 $\mathcal{E}$ 到 $\mathcal{S}$ 的一个几何态射 $\Gamma: \mathcal{E} \longrightarrow \mathcal{S}, \Gamma(\Gamma^* \dashv \Gamma_*)$). $\mathcal{S}$ 不一定是抽象集合的范畴，但 $\mathcal{S}$ 一般是 Boolean 的. $\mathcal{E}$ 作为一个空间的范畴应该满足：

1. 几何态射 $\mathcal{E} \xrightarrow{\Gamma} \mathcal{S}\left(\mathcal{E} \underset{\Gamma_*}{\overset{\Gamma^*}{\rightleftarrows}} \mathcal{S}\right)$ local, 即 $\Gamma_*$ 具有一个 right adjoint $\Gamma^!$:

$$\mathcal{E} \quad \begin{array}{c} \xleftarrow{\Gamma^*} \\ \xrightarrow[\Gamma_*]{} \\ \xleftarrow[\Gamma^!]{} \end{array} \quad \mathcal{S}$$

可以认为 $\Gamma^*$ 是离散空间的子范畴嵌入于"全体"空间的范畴 $\mathcal{E}$. $\Gamma^!$ 是 chaotic 空间即非离散空间的子范畴嵌入于 $\mathcal{E}$. 而 $\Gamma_*$ 是函子 $\mathrm{pts}(\ ) = \mathcal{E}(1, _)$. 当然对于不同的 $\mathcal{E}$, 离散与 chaotic 有不同的含义.

2. $\mathcal{E} \xrightarrow{\Gamma} \mathcal{S}$ essential, 即 $\Gamma^*$ 具有一个 left adjoint $\Gamma_! = \pi_0$; 而且要求 $\pi_0$ 保持有限乘积 (finite products).

$$\mathcal{E} \underset{\Gamma^{!}}{\overset{\Gamma_! = \pi_0}{\underset{\Gamma_*}{\overset{\Gamma^*}{\rightleftarrows}}}} \mathcal{S}$$

$\Gamma_! = \pi_0$ 经常称为"连通分支函子"(connected components).

如果 $M$ 是一个拓扑空间, $K$ 是任一集合, 我们有如下自然一一对应:

$$\begin{array}{c} \pi_0(M) \longrightarrow K \\ \hline M \longrightarrow \mathrm{dis}(K) \end{array},$$

$\pi_0(M)$ 是 $M$ 的连通分支构成的集合.

这条公理对于构造 homotopy— 从量到质, 是必要的:

由于 $\pi_0$ 保持有限乘积, $\pi_0$ 同 $\Gamma_*$ 一样也是一个闭函子, 即 $\pi_0$ 可以把 $\mathcal{E}$–enriched 范畴送到 $\mathcal{S}$–enriched 范畴.

因为 $\mathcal{E}$ 是 cartesian closed, 所以 $\mathcal{E}$ 可以看成一个 $\mathcal{E}$–enriched 范畴. 即定义两个对象 $X,Y$ 之间的态射为 $Y^X$, $Y^X$ 仍是一个 $\mathcal{E}$–空间. ($Y^X$ 的点 $\mathcal{E}(1,Y^X) \approx \mathcal{E}(X,Y)$). 通过 $\pi_0$, $\mathcal{E}$ 过渡到它的 homotopy 范畴 $[\mathcal{E}]$, $[\mathcal{E}]$ 是 $\mathcal{S}$–enriched 的范畴. 它具有与 $\mathcal{E}$ 相同的对象. 但对任意两个 $\mathcal{E}$- 空间 $X,Y$, 定义 $[\mathcal{E}](X,Y) = \pi_0(Y^X)$. $\pi_0(Y^X)$ 是函数空间 $Y^X$ 的连通分支的"集合", 即 $X$ 到 $Y$ 的态射的 homotopy classes.

正像定义拓扑空间 $X$ 到 $Y$ 的连续映射的 homotopy classes 一样, 从 $X$ 到 $Y$ 的两个连续映射 $f,g$ 属于同一个 homotopy class, 仅当存在空间 $Y^X$(用 $Y^X$ 表示 $X$ 到 $Y$ 的连续函数构成的空间) 上

的一个 path $F$, 即一个从单位区间 $I$ 到 $Y^X$ 的连续映射 (注意, $I$ 到 $Y^X$ 的连续态射 $F$, 一般等同于一个从 $I \times X$ 到 $Y$ 的连续映射 $\overline{F}: I \times X \longrightarrow Y$). 满足条件: $F(0) = f$, $F(1) = g$ 或 $\overline{F}(0, x) = f(x)$, $\overline{F}(1, x) = g(x)$. 即 $f, g$ 属于同一连通分支 (path 连通分支).

对于态射的 composition, $Y^X \times Z^Y \longrightarrow Z^X$(这是 $\mathcal{E}$ 中的 evaluation). 因为 $\pi_0$ 保持有限乘积, 这样我们有一个同构 (isomorphism): $\pi_0(Y^X) \times \pi_0(Z^Y) \xrightarrow{\sim} \pi_0(Y^X \times Z^Y)$. $\pi_0$ 把 $\mathcal{E}$ 中的 composition (evaluation) 送到相应的 $\mathcal{S}$ 中的 composition (evaluation):

$$\pi_0(Y^X) \times \pi_0(Z^Y) \xrightarrow{\sim} \pi_0(Y^X \times Z^Y) \longrightarrow \pi_0(Z^X).$$

**注 1** 函子范畴 $\mathcal{E} = \mathcal{S}^{\mathbf{C}^{op}}$ 是一个 $\mathcal{S}$-topos, 即存在几何态射 $\Gamma: \mathcal{S}^{\mathbf{C}^{op}} \longrightarrow \mathcal{S}$. 如果 $\mathcal{S}$ 是抽象集合的范畴, $\Gamma^*: \mathcal{S} \longrightarrow \mathcal{S}^{\mathbf{C}^{op}}$ 通常记为 $\Delta$. 对任意抽象集合 $X$, $\Gamma^*(X) = \Delta X$ 是一个常函子, 对 $\mathbf{C}$ 的任一对象 $C$, $\Delta X(C) = X$. $\Gamma_*: \mathcal{E} = \mathcal{S}^{\mathbf{C}^{op}} \longrightarrow \mathcal{S}$, $\Gamma_* = \varprojlim$. $\Gamma^*$ 有一个 left adjoint $\Gamma_! = \varinjlim = \pi_0$, 但是 $\varinjlim$ 一般并不保持有限乘积. 如果 $\mathbf{C}$ 有 terminal object 1, 那么 $\Gamma_* = \varprojlim$ 是对 1 的 evaluation $\mathrm{ev}_1$: 让 $F$ 是 $\mathcal{S}^{\mathbf{C}^{op}}$ 的一个对象, $\varprojlim F = F(1)$. 1 所代表的函子 $\mathbf{C}(_, 1)$ 是 $\mathcal{S}^{\mathbf{C}^{op}}$ 的 terminal 对象. 这样 $F(1) = \mathcal{S}^{\mathbf{C}^{op}}(1, F)$ =pts($F$).

特别, 这时 $\Gamma_*$ 有一个 right adjoint $\Gamma^!$. 让 $X$ 是一个抽象集合, 那么 $\Gamma^!(X) = X^{\mathbf{C}(1,_)}$.

$$\mathcal{S}^{\mathbf{C}^{op}} \quad \begin{array}{c} \Gamma! = \pi_0 = \varinjlim \\ \longrightarrow \\ \Gamma^* = \Delta \\ \longleftarrow \\ \longrightarrow \\ \Gamma_* = \varprojlim = \mathrm{ev}_1 \\ \longleftarrow \\ \Gamma! = (\ )^{\mathbf{C}(1,-)} \end{array} \quad \mathcal{S}$$

**注 2** 如果 $\mathbf{C} = G$ 是一个群，那么 $\mathcal{S}^{\mathbf{C}^{op}} = \mathcal{S}^{G^{op}}$ 是右 $G$- 集的范畴. 我们有 $\pi_0(G) = 1$, 但是 $\pi_0(G \times G) = G$. 这样，$\pi_0$ 不保持有限乘积.

3. $\pi_0(\Omega) = 1$.

这里 $\Omega$ 是 truth value object. 这就是说，$\Omega$ 是连通的. 对 $\mathcal{E}$-空间 $X$, 我们有 $[\mathcal{E}](X, \Omega) = \pi_0(\Omega^X) = 1$, 即 $X$ 的所有"子空间"组成的空间 $\Omega^X$ 也是连通的，或说 contractible. 从 $X$ 到 $\Omega^X$ 有一个自然嵌入 $X \hookrightarrow \Omega^X$. 这样，任一空间 $X$ 可以自然嵌入到一个 contractible 空间.

这一条对于任一 Boolean topos 是不对的. 因为对一个 Boolean topos, $\Omega \approx 1 + 1$, 而 $\pi_0$ 保持 colimits, 那么 $\pi_0(\Omega) \approx \pi_0(1) + \pi_0(1) = 1 + 1$.

一个满足以上这三个条件的 topos 的简单例子如下：取 $\mathbf{\Delta}_1$ 是由从 $\{0, 1 \mid 0 \le 1\}$ 到 $\{0, 1 \mid 0 \le 1\}$ 的所有保序映射构成的 monoid. 那么 $\mathbf{\Delta}_1$ 有三个元素：恒等映射 $1_{\mathbf{\Delta}_1}$, 常映射 0 和 1. 分别记为 $1, \partial_0, \partial_1$. 满足条件 $\partial_i \partial_j = \partial_i$, $i, j = 0, 1$. 做函子范畴 $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$, $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 是右 $\mathbf{\Delta}_1$- 集. $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 满足以上三个条件. $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 的对象 $X$ 可以简单看成 graph:

对 $x \in X$, 我们有 $x\partial_0 \xrightarrow{x1 = x} x\partial_1$

即可以认为 $x$ 是一个箭头，具有起点 $x\partial_0$, 终点 $x\partial_1$. 如果 $x\partial_0 = x\partial_1$, 那么 $x$ 是一个 loop $x\partial_0 = x\partial_1 \circlearrowleft x$；如果 $x\partial_0 = x\partial_1 = x$, 那么 $x$ 是一个固定点 (fixed point). $\mathcal{S}^{\mathbf{\Delta}_1^{op}}$ 的 truth value object $\Omega = \cdot \rightleftarrows \cdot \circlearrowright$, $\Omega$ 是连通的.

## §3 空间和量

Lawvere 说："We are in the world, we can move ourselves in

the world and hence the world is reflected in us. In our thinking we struggle to create an image of the world and in particular an image of ourselves in our thinking process. These two components of the scientific struggle are called by Grassmann 'real' science and 'formal' science, the science of things and thoughts."

"The fact that we are in the world and can move ourselves in the world is called 'space'. The resulting reflections in thinkings are called 'number' and the result of this fundamental relationship including measuring can be studied in more detail by means of both pure mathematics and dialectics."

作为空间的范畴，如拓扑空间构成的范畴或作为一个广义空间的范畴，如一个拓扑空间 $X$ 上 sheaf. $\mathrm{Sh}(X)$ 应该是 topos. 但在这里，我们讨论这两类空间范畴 (统称为空间范畴) 所应具备的最初步、最基本的性质 (上一节我们讨论了它们的不同点); 以及作为量、数量的范畴所应具备的基本性质; 空间范畴和量的范畴的联系.

空间范畴 $\mathbf{D}$ 应该具有有限极限 (limits) 和上乘积 (coproducts). 任意一个具有乘积与上乘积的范畴，$A, B, C$ 是任意三个对象，存在一个典型 (canonical) 态射

$$(A \times B) + (A \times C) \longrightarrow A \times (B + C).$$

这个态射一般不是同构.

作为空间范畴 $\mathbf{D}$, 则要求这个典型态射是一个同构，也就是说分配律成立.

对于任一 $\mathbf{D}$- 空间 $X$, $\mathbf{D}/X$ 是空间 $X$ 上的 bundle 做成的范畴. 通常称为逗号范畴 (comma category), 因为 $\mathbf{D}/X$ 常记为 $(\mathbf{D}, X)$. $\mathbf{D}/X$ 中的对象都是以 $X$ 为 codomain 的 $\mathbf{D}$ 中态射. $A \xrightarrow{a} X$,

$\mathbf{D}/X$ 的一个态射是一个可换三角形 $\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {}_a\searrow \quad \swarrow_b & \\ & X & \end{array}$, $a = bf$.

$\mathbf{D}/X$ 具有乘积与上乘积. $\mathbf{D}/X$ 中的乘积是 $\mathbf{D}$ 中的 pullback; 而 $\begin{array}{c} A \\ \downarrow \\ X \end{array} + \begin{array}{c} B \\ \downarrow \\ X \end{array} = \begin{array}{c} A+B \\ \downarrow \\ X \end{array}$.

我们要求对任一 $\mathbf{D}$- 空间 $X$. $\mathbf{D}/X$ 也满足分配律.

另外两个条件:

$\mathbf{D}/0 \approx \mathbf{1}$. $\mathbf{1}$ 是只有一个对象及一个恒等态射的范畴, 以及上乘积的不交性 (disjointness of coproduct): $\begin{array}{c} X \\ \downarrow \\ X+Y \end{array}$ 和 $\begin{array}{c} Y \\ \downarrow \\ X+Y \end{array}$ 的交 (即它们的 pullback) $\begin{array}{ccc} 0 & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X & \longrightarrow & X+Y \end{array}$ 是空的 (同构于 initial object), 这与 $\mathbf{D}/X \times \mathbf{D}/Y \xrightarrow{\sim} \mathbf{D}/(X+Y)$ 等价.

一个范畴 $\mathbf{D}$ 满足以下四条:

(1) $(A \times B) + (A \times C) \xrightarrow{\sim} A \times (B + C)$;

(2) 对任意 $\mathbf{D}$- 空间 $X$, $\mathbf{D}/X$ 也满足 (1);

(3) $\mathbf{D}/0 \xrightarrow{\sim} \mathbf{1}$;

(4) $\mathbf{D}/X \times \mathbf{D}/Y \xrightarrow{\sim} \mathbf{D}/(X+Y)$,

称为分配范畴 (distributive category).

这是作为空间范畴所应具有的最基本性质 (当然 topos 是分配范畴).

两个拓扑空间的乘积即乘积拓扑, 上乘积是不交并. 拓扑空间和连续映射的范畴 Top 满足以上四条, 因而是一个分配范畴, 虽然 Top 不是一个 topos.

作为量和数量的范畴 $\mathbf{L}$, 应具有有限乘积与上乘积, 它的最基本性质是线性性.

(1) $0 \simeq 1$, initial object 和 terminal object 同构. 例如在 $R$- 模构成的范畴 $R$-mod 内, initial 和 terminal object 都是 0 模, 这里

$R$ 是一个环.

马上可以看到，这个条件是任何一个非平凡 (nontrivial) 分配范畴所不能满足的，因为对任意范畴 $\mathbf{D}$, $\mathbf{D}/1 \approx \mathbf{D}$.

从上乘积到乘积的态射 $\sum_{i\in I} A_i \xrightarrow{f} \prod_{j\in J} B_j$ 由一个 $n\times m$ 矩阵 $(f_{ij})_{n\times m}$ 组成，这里 $^{\#}I = n$, $^{\#}J = m$.

$$\begin{array}{ccc} \sum_{i\in I} A_i & \xrightarrow{f} & \prod_{j\in J} B_j \\ \uparrow & & \downarrow \\ A_i & \xrightarrow{f_{ij}} & B_j \end{array}$$

任意两个对象 $A, B$ 之间存在一个态射 $0_{AB}$:

$$A \longrightarrow 1 \xrightarrow{\sim} O \longrightarrow B, \qquad 0_{AB}: A \to B$$

这样我们可以构造一个从 $A+B$ 到 $A\times B$ 的典型态射

$$A+B \xrightarrow[\begin{pmatrix} 1_A & 0_{AB} \\ 0_{BA} & 1_B \end{pmatrix}]{} A\times B.$$

第二个条件，要求这个典型态射是一个同构.

(2) $A+B \xrightarrow[\begin{pmatrix} 1_A & 0_{AB} \\ 0_{BA} & 1_B \end{pmatrix}]{} A\times B$ 是一个同构.

满足这两条的范畴 $\mathbf{L}$ 称为线性范畴 (linear category).

例如范畴 $R$-mod(若 $R$ 是一个域， $R$-mod=Vect$_R$, $R$ 上向量空间的范畴) 是一个线性范畴． $R$-mod 内的乘积称为直积 (direct product), 上乘积称为直和 (direct sum). 对于有限个 $R$- 模, $A_1, \cdots, A_n$, 它们的直积与直和是一致的,

$$\prod_{i=1}^{n} A_i \approx \sum_{i=1}^{n} A_i.$$

这样在一个线性范畴 $\mathbf{L}$ 内，有限乘积与上乘积是一致的．它们常常被称为 biproduct, 表示为 $A \oplus B$.

$A$ 是 $\mathbf{L}$ 的一个对象， $A + A \xrightarrow{\nabla_A} A$ 是 codiagonal, 即

$$\begin{array}{ccc} A & & \\ {\scriptstyle i_A}\downarrow & \searrow^{1_A} & \\ A+A & \xrightarrow{\nabla_A} & A. \\ {\scriptstyle i_A}\uparrow & \nearrow_{1_A} & \\ A & & \end{array}$$

定义 $A \times A \xrightarrow{+} A$ 为态射 $A \times A \xrightarrow{\sim} A + A \xrightarrow{\nabla_A} A$ 的复合.

那么二元运算 + 是可交换，可结合的， $0_A : 1 \longrightarrow A$ 是单位元 (neutral element)．这样， $A$ 是一个可换 monoid 对象．并且 $\mathbf{L}$ 中的态射 $f$ : $A \longrightarrow B$ 保持 +, 即以下方形可换：

$$\begin{array}{ccc} A \times A & \xrightarrow{+} & A \\ \downarrow{\scriptstyle f\times f} & & \downarrow{\scriptstyle f} \\ B \times B & \xrightarrow{+} & B \end{array}$$

$\mathbf{L}$ 中的任一对象 $L$ 到 $A$ 的全体态射 $\mathbf{L}(L, A)$ 成为一个通常意义下的可换 monoid: 对于 $f, g \in \mathbf{L}(L, A)$, $L \underset{g}{\overset{f}{\rightrightarrows}} A$, 定义 $f + g = + \circ (f, g)$.

$$\begin{array}{ccc} L & \xrightarrow{(f,g)} & A \times A \\ & \searrow_{f+g} & \downarrow{\scriptstyle +} \\ & & A \end{array}$$

$\mathbf{L}(L, A)$ 具有单位元 $0_{LA}$： $L \longrightarrow 1 \xrightarrow{\sim} 0 \longrightarrow A$.

可以认为 $\mathbf{L}(L, A)$ 是一个量或数量系统，就像 $\mathbf{L}(1, \mathbf{R})$ 是一个数量系统一样，这里 $\mathbf{R}$ 是实数对象.

复合 (compose) 态射 $\alpha$： $L' \longrightarrow L$ 于 $(f, g)$, $(f, g) \circ \alpha$ 给我们一个从 monoid $\mathbf{L}(L, A)$ 到 monoid $\mathbf{L}(L', A)$ 的同态；同样一个态射 $\beta$： $A \longrightarrow A'$. 导致从 $\mathbf{L}(L, A)$ 到 $\mathbf{L}(L, A')$ 的同态. 这样态射 $\alpha, \beta$ 导致不同量、数量系统之间的同态.

空间范畴是分配范畴；量，数量的范畴是线性范畴. 那么空间与数量的关系如何体现这两类范畴的关系呢？

首先，一条重要的原则是：

一个数量系统是一个空间.

一个线性范畴 $\mathbf{L}$ 通常 enrich 于一个给定的分配范畴 $\mathbf{D}$, 这就是说，存在一个 bifunctor $\mathbf{L}$(同样表示为 L),

$$\mathbf{L}: \mathbf{L}^{\mathrm{op}} \times \mathbf{L} \longrightarrow \mathbf{D}.$$

$A, B$ 是 $\mathbf{L}$ 的对象， $\mathbf{L}(A, B)$, $A$ 到 $B$ 的态射，是一个 $\mathbf{D}$- 空间.

Composition law 是一个 $\mathbf{D}$ 的一个态射：

$$\mathbf{L}(A, B) \times \mathbf{L}(B, C) \longrightarrow \mathbf{L}(A, C).$$

1 是 $\mathbf{D}$ 的 terminal object. 我们有自然一一对应 (natural bijection):

$$\frac{1 \longrightarrow \mathbf{L}(A, B)}{A \longrightarrow B}$$

即 $\mathbf{L}$ 中 $A$ 到 $B$ 的态射一一对应于 $\mathbf{D}$ 中空间 $\mathbf{L}(A, B)$ 的点.

Lawvere 说："Such an enrichment is precisely the fundamental structure of functional analysis, because it gives a determined meaning to continuous variations, smooth parametrization, and approximations within systems of numbers all of which can be explained

and studied in terms of D–morphisms

$$T \longrightarrow \mathbf{L}(A,B)$$

where $T$ is an appropriately chosen D–space other than the point 1."

线性范畴 $\mathbf{L}$ 的对象应该看成量的类，而态射 $A \longrightarrow B$ 是一个 $\frac{A}{B}$ 类的量. 几何上，量的类可以是简单的线性维数，或是各种类的张量丛 (tensor bundles); 在物理上，它们可以是质量，长度，时间，压力，能量等等. 存在很多特殊的空间，比如可以用代数表示的，如果空间 $Y$ 有环结构，我们常常结合 $Y$ 上全体有限生成射影模 (finitely–generated projective $Y$–modules) 的范畴 $\mathbf{P}(Y)$.

更一般地说，一个空间上的量和数量系统应构成一个线性范畴：D 为空间范畴即一个分配范畴，R 是一个小的线性范畴，R enrich 于 D, R 可以看为 D– 空间的量的值域. 对任一 D– 空间 $X$, $\mathbf{D_R}(X)$ 是 $X$ 上量系统的线性范畴，$\mathbf{D_R}(X)$ 具有与 R 相同的对象，但两个对象 $A, B$ 之间的态射是 D 中态射 $X \longrightarrow \mathbf{R}(A,B)$.

于是我们得到一个基本上可以代表的函子 (an essentially representable functor):

$$\mathbf{D_R}(\ ):\ \mathbf{D}^{op} \longrightarrow \text{Lin Cat}\quad (\text{linear categories})$$

$$\mathbf{D_R}(X)(A,B) = \mathbf{D}(X, \mathbf{R}(A,B)).$$

$\mathbf{D_R}(\ )$ 具有性质

$$\mathbf{D_R}(1) = \mathbf{R};$$

$$\mathbf{D_R}(0) = \{0\};$$

$$\mathbf{D_R}(X+Y) = \mathbf{D_R}(X) \times \mathbf{D_R}(Y).$$

对每一个 D–epimorphism $X \longrightarrow Y$, 有一个忠实线性函子

$$\mathbf{D_R}(Y) \hookrightarrow \mathbf{D_R}(X).$$

## §4 Intensive 和 extensive quantities

Lawvere 教授在 1987 年春天开了一门课 "Algebraic concepts in the foundations of Physics and Engineering". 他引用著名物理学家 J. C. Maxwell 1871 年 3 月 9 日 (他的著名电磁学的方程发表于此一年之前) 给 London Mathematical Society 的文章 "Remarks on the mathematical classification of physical quantities" 中下列的话:

"The first part of the growth of a physical science consists in the discovery of a system of quantities on which its phenomena may be conceived to depend. The next stage is the discovery of the mathematical form of the relations between these quantities. After this the science may be treated as a mathematical science, and the verification of the laws is effected by a theoretical investigation of the conditions under which certain quantities can be most accurately measured, followed by an experimental realization of these conditions, and actual measurement of the quantities.

It is only through the progress of science in recent times that we have become acquainted with so large a number of physical quantities that a classification of them is desirable.

One very obvious classification of quantities is founded on that of the sciences in which they occur. Thus temperature, pressure, density, specific heat, latent heat, etc., are quantities occuring in the theory of the action of heat on bodies.

But the classification which I now refer to is founded on the mathematical or formal analogy of the differenr quantities, and not on the matter to which they belong. Tbus a finite straight line,

a force, a velocity of rotation, etc., are quantities differing in their physical nature, but agreeing in their mathematical form. We may distinguish the two methods of classification by calling the first a physical, and the second a mathematical classification of quantities.

A knowledge of the mathematical classification of quantities is of great use both to the original investigator and to the ordinary student of the science.

... The most obvious case is that in which we learn that a certain system of quantities in a new science stands to one another in the same mathematical relations as a certain other system in an old science, which has already been reduced to a mathematical form, and its problems solved by mathematicians.

But it is evident that all analogies of this kind depend on principles of a more fundamental nature; and that, if we hed a true classification of quantities, we should be able at once to detect the analogy hetween any system of quantities in known sciences, so that we should lose no time in availing ourselves of the mathematical labours of those who had already solved problems essentially the same.

Position and form, which were formerly supposed to be in the exclusive possession of geometers, were reduced by Descartes to submit to the rules of arithmetic by means of that ingenious scaffolding of coordinates axes which he made the basis of his operations.

Since this great step was taken in mathematics, all quantities have been treated in the same way, and presented to the mind by means of numbers, or symbols which denote numbers, so that as soon as any science has been thoroughly reduced to the mathematical form, the solution of problems in that science, as a mental process,

is supposed (at least by the outer world) to be carried on without the aid of any of the physical ideas of the science.

I need not say that this is not true, and mathematicians in solving physical problems, are very much aided by a knowledge of the science in which the problems occur.

At the same time, I think that the progress of science, both in the way of discovery and in the way of diffusion, would be greatly aided if more attention were paid in a direct way to the classification of quantities.

A most important distinction was drawn by Hamilton when he divided the quantities with which he had to do into Scalar quantities, which are completely represented by one numerical quantity, and Vectors, which require three numerical quantities to define them.

The invention of the calculus of Quaternions is a step towards the knowledge of quantities related to space which can only be compared, for its importance, with the invention of triple coordinates by Descartes. The ideas of this calculus, as distinguished from its operations and symbols, are fitted to be of the greatest use in all parts of science.

We may imagine another step in the advancement of science to be the invention of a method, equally appropriate, of conceiving dynamical quantities. As our conceptions of physical science are rendered more vivid by substituting for the more numerical ideas of Cartesian mathematics the geometrical ideas of Hamiltonian mathematics, so in the higher sciences the ideas might receive a still higher development if they could be expresses in a language as appropriate to dynamics as Hamilton's is to geometry."

Lawvere 说: "Any specific space will have variable quantities.

In fact, for many purposes in mathematics, that is the main reason why we have spaces as domain of variation. Why are there different spaces? Because there are different degrees or qualities of variation of quantities that are possible. So, a space is a domain of variation for quantities. But then, different kinds of variation are possible over that particular domain space. Different kinds of quantities, and this is the kind of classification that Maxwell refers to; classification that has many dimensions, many directions."

Lawvere 教授提出划分量和数量 (不仅仅是物理量) 为 intensive 和 extensive quantities. 他说，这两个概念自中世纪就有，它们甚至出现在黑格尔的哲学著作中，但不知为什么只有在热动力学中提到它们.

下面是 intensive 和 extensive quantities 在物理学中的一些例子：

| Intensive | Extensive | Intensive | Extensive |
|---|---|---|---|
| 体积 | 特殊体积 | 电荷 | 特殊电荷 |
| 能量 | 特殊能量 | 力 | 压力 |
| 质量 | 质量密度 | 热量 | 温度 |
| 熵 | 特殊熵 | | |

这里 "特殊" 是指 "每单位质量"，如特殊体积 — 每单位质量体积.

一般来说， intensive quantities 是 extensive quantities 的比值. 当然有时有的 intensive quantities 被当作基本的，比如压力.

Extensive quantities 是与空间有关的 (extension)，它们与空间的度量有关. 有的人说，如果你把一个质量 (mass) 分成两半，那么 extensive quantities 也分成两半，而 intensive quantities 却不然.

Extensive quantities 具有加法，并且有数乘. Intensive quantities 不仅可加，可被数乘，并且具有乘法. 一个空间上的 intensive quantities 通常形成一个代数，而 extensive quantities 形成一个模.

Extensive quantities 是协变的 (covariant)，而 intensive quantities 是反变的 (contravariant).

例如 $X$ 是一个拓扑空间. 取 $X$ 上的 Radon measures with compact support 为 extensive quantities，记为 $\mathfrak{M}(X)$. $X$ 上的 intensive quantities 是 $X$ 上的全体实值连续函数，表示为 $C(X)$. $\mathbf{R}$ 是实数，则 $\mathfrak{M}(X)$ 是一个 $\mathbf{R}$- 模，而 $C(X)$ 是一个 $\mathbf{R}$- 代数. 如果 $f$ 是一个从空间 $X$ 到空间 $Y$ 的一个连续函数，$f$ 导致 $f_! : \mathfrak{M}(X) \longrightarrow \mathfrak{M}(Y)$, $f_!(\mu)(B) = \mu(f^{-1}(B))$，这里 $\mu \in \mathfrak{M}(X)$, $B$ 是 $X$ 的一个可度量子集 (measurable set)；并且 $f$ 还导致 $f^* : C(Y) \longrightarrow C(X)$，对于 $g \in C(Y)$, $f^*(g) = g \circ f \in C(X)$.

当然 quantities 的值不应当只是一维常数，quantities 的值应当具有维数，它们应该也构成一个范畴. 如前面提到的结合于空间范畴 $\mathbf{D}$ 的线性范畴 $\mathbf{R}$，可以是 $\mathbf{D}$- 空间上的 quantities 的值构成的范畴.

这里为简单起见，我们只考虑以一维常量为值的 quantities.

这样 $\mathfrak{M}$ 以及 $C$ 成为从拓扑空间的范畴 Top 到线性范畴 $\mathbf{L}$(例如 $\mathbf{L} = \mathbf{R}$-mod) 的函子. Intensive quantities 函子 $C$ 是可代表的 (representable)，由实数空间 $\mathbf{R}$ 代表，即对任一拓扑空间 $X$, $C(X) = \mathrm{Top}(X, \mathbf{R})$. $\mathfrak{M}$ 是 Top 到 $\mathbf{L}$ 的协变函子，而 $C$ 是 Top 到 $\mathbf{L}$ 的反变函子.

Extensive quantities 具有总量 (total value). 因为 $\mathbf{D}$ 中有 terminal object 1，从任一 $\mathbf{D}$- 空间 $X$ 到 1 有唯一态射，记为 $X : X \longrightarrow 1$. 这个唯一态射导致 extensive quantities 的总量. 例如 $\mathbf{D} = \mathrm{Top}$:

$$\begin{aligned} \mathfrak{M}(X) &\longrightarrow \mathfrak{M}(1) = \mathbf{R} \\ \mu &\longmapsto \mu(X) \in \mathbf{R} \end{aligned}$$

而对 intensive quantities, 这个唯一态射 $X: X \longrightarrow 1$ 导致 $\mathbf{R} = \mathcal{C}(1) \longrightarrow \mathcal{C}(X)$, 即常函数的嵌入.

对于 extensive quantities $\mathfrak{M}, X$ 的点 $x: 1 \longrightarrow X$ 导致一个所谓的 Dirac 函数 $\delta_x$,

$$\begin{aligned} \delta_x: \mathbf{R} = \mathfrak{M}(1) &\longrightarrow \mathfrak{M}(X) \\ r &\longmapsto r\delta_x \end{aligned}$$

$$r\delta_x(B) = \begin{cases} r, & \text{若 } x \in B \\ 0, & \text{若 } x \notin B \end{cases}.$$

而对 intensive quantities $\mathcal{C}$, $x: 1 \longrightarrow X$ 导致 evaluation 函数 $\mathrm{ev}_x$,

$$\begin{aligned} ev_x: \mathcal{C}(X) &\longrightarrow \mathcal{C}(1) = \mathbf{R} \\ f &\longmapsto ev_x(f) = f(x). \end{aligned}$$

Extensive quantities 和 intensive quantities 之间有一种 bilinear pairing 关系. 这种关系对不同的空间范畴 $\mathbf{D}$ 有不同的具体解释. 例如 $\mathbf{D}$ =Top. 对拓扑空间 $X$, 这种 bilinear pairing 关系是一个 bilinear 映射:

$$\begin{aligned} \mathfrak{M}(X) \times \mathcal{C}(X) &\longrightarrow \mathbf{R} \\ (\mu, f) &\longmapsto \int_X f\, d\mu. \end{aligned}$$

更进一步, $\mathfrak{M}(X)$ 是一个 $\mathcal{C}(X)$- 模:

$$\begin{aligned} \mathfrak{M}(X) \times \mathcal{C}(X) &\longrightarrow \mathfrak{M}(X) \\ (\mu, f) &\longmapsto \mu \cdot f \end{aligned}$$

对 $X$ 的一个可度量子集 $B$, $\mu \cdot f(B) = \int_B f\, d\mu$.

对拓扑空间 $X$, 我们取 intensive quantities 为 $\mathcal{C}(X) = \mathrm{Top}(X, \mathbf{R})$, 在范畴 Top 内没有任何限制; 而对 extensive quantities $\mathfrak{M}(X)$ 限制

为 Radon measures with compact support. 这样，这种模结构 (module structure) 就很自然. 如果像不少教科书那样 (例如 Bourbaki) 限制 $C(X)$ 为有 compact support 的连续函数，而对 $\mathfrak{M}(X)$ 却没有任何限制，这样，这种模结构的存在是一个真正的问题.

在这些书中，要求两个空间之间的映射必须是 proper, 即紧集 (compact set) 的逆象仍是紧的 (但一般连续函数并不满足这一条). 这样，intensive quantities 将不可代表, 而空间范畴将没有 terminal object, 因为 $X \longrightarrow 1$ 是 proper 仅当 $X$ 是紧的.

一个空间 $X$ 上的 extensive quantities 并不一定都是集函数 (定义在 $X$ 的子集上的函数). 例如在微分几何中，$C^\infty$ 表示由 smooth manifolds ($C^\infty$- 空间) 以及 $C^\infty$- 映射构成的范畴. $C^\infty$ 在物理学中比范畴 Top 有更多的应用. 一个 $C^\infty$- 空间 $X$ 上的 extensive quantities 可以取 $X$ 上的 currents, 而 intensive quantities 则是 $X$ 上的 differential forms. Currents 和 differential forms 都是有维数 (dimension) 的.

$X$ 上的一个 $\mathbf{R}$ 值 differential $n$–form $w$ 是一个 fibrewise multilinear alternating map

$$w: TX \times_X TX \times \cdots \times_X TX \longrightarrow \mathbf{R}$$

这里 $TX$ 是 $X$ 的 Tangent space, $TX \times_X TX \times \cdots \times_X TX$ 是 $TX \longrightarrow X$ 的 $n$–fold pullback.

用 $E^n(X)$ 表示 $X$ 上 $\mathbf{R}$ 值 differential $n$–form, $E^n(X)$ 是一个 $\mathbf{R}$- 模 (实际上是一个 $\mathbf{R}$- 代数).

$X$ 上的一个 $\mathbf{R}$- 值 $n$-(compact) current $\gamma$ 是一个 $\mathbf{R}$- 线性映射 $\gamma: E^n(X) \longrightarrow \mathbf{R}$.

用 $E_n(X)$ 表示 $X$ 上 $\mathbf{R}$ 值 $n$–currents, $E_n(X)$ 是一个 $\mathbf{R}$- 模. 对任意 $n$, $E^n(\ )$ 和 $E_n(\ )$ 是从范畴 $C^\infty$ 到范畴 $\mathbf{L} = \mathbf{R}$–mod 的函子，$E^n(\ )$ 是反变函子，而 $E_n(\ )$ 是协变函子.

$E_n(X)$ 是一个 $E^n(X)$ 模. 让 $\gamma$ 为一个 $n$-current; $w, v$ 为 differential $n$-form. 那么 $\gamma \cdot w$ 是一个新的 $n$-current, 即是一个从 $E^n(X)$ 到 $\mathbf{R}$ 的 $\mathbf{R}$- 线性映射.

$$\gamma \cdot w(v) = \gamma(wv)$$

因为 $E^n(X)$ 是一个 $\mathbf{R}$- 代数，所以两个 differential forms 的乘积 $wv$ 仍是一个 differential form.

通常用积分表示 current 和 differential forms 之间的 bilinear pair relation:

$$\begin{array}{ccc} E_n(X) \times E^n(X) & \longrightarrow & \mathbf{R} \\ (\gamma, w) & \longmapsto & \gamma(w) = \int_\gamma w \end{array}$$

同样，homology 是 extensive quantity 而 cohomology 是 intensive quantity, homology 是协变的， cohomology 是反变的． 1943 年， Eilenburg 和 MacLane 证明了 cohomology 在 homology 范畴内是可以代表的，即由 Eilenburg–MacLane spaces $K[\pi, n]$ 代表，

$$H^n(X, \pi) \simeq [X, K[\pi, n]].$$

以 Lawvere 教授为代表的一批数学家对什么是数学基础，以及为什么要研究数学基础是非常明确的.

数学基础必须为一切需要数学的专业人员服务，为澄清和简化他们的学习、发展和应用数学的过程服务.

他们提出的观点，理论很多尚不完善，处于发展探索阶段. 但是这些理论的重要性正在逐渐被人们所认识.

几年前， Schanuel 教授在他的课上讲解 Lawvere 关于微分几何学的一些观点理论时说到，我们并不期望去说服我们的祖父们，叔叔们去理解这些理论，但是我们的儿子们和孙子们将会学习研究这些对他们来说习以为常的观点以及理论.

# 参考文献

1 Kock A. Synthetic Differential Geometry. Cambridge: Cambridge Univ. Press, 1981

2 Lawvere F W. An elementary theory of the category of sets. Proc. National Acad. Sci. U.S.A., 1964, 52: 1506~1511

3 Lawvere F W. Adjointness in foundations. Dialectica, 1969, 23: 281~296

4 Lawvere F W. Metric spaces, generalized logic and closed categories. Rend. Sem. Mat. Fis. Milano, 1973, 43: 135~166

5 Lawvere F W. Continuously variable sets: algebraic geometry = geometric logic. Logic Colloquium'73 (edited by Rose H E and Shepherdson. J C ) Amsterdam: North-Holland Publ. Co., 1975, 135~156

6 Lawvere F W. Toward the description in a smooth topos of the dynamically possible motions and deformations of a continuous body. Cahiers Topologie Géom Différentielle, 1980, 21: 377~392

7 Lawvere F W. Introduction to categories in continuum physics. Lecture Notes in Math., 1986, 1174: 1~16

8 MacLane S. Categories for the Working Mathematician. Heidelberg: Springer-Verlag, 1971

# 第 21 章

# Topos 理论以及范畴论的哲学意义

70 年代初 Lawvere, Tierney 提出 topos 的概念， 20 多年来 topos 理论和与其相关的领域有很大发展. 其重要意义被越来越多的人认识到. 各家出来给以不同的解释. 一种流行的观点是 topos 理论是集合论的延伸和扩展，它为直觉逻辑提供了模型. 这种观点只说明了 topos 理论在一方面的作用. 若认为 topos 理论的起源是为了推广集合论 (如 Goldblatt, 《 Topoi 》), 那就是错误的了. Colin McLarty 在 1990 年英国哲学科学杂志上有一篇文章对这一问题做了专门论述 [3].

Topos 理论的哲学意义在于把 “变化” 直接引入数学. 通常集合的范畴是常量的范畴，而一个 topos 是具有某种内结构的变化的空间或量的 “集合” 的范畴. 这就为直接地更深刻更精确地描述客观物质世界，为物理学提供了更有效的数学模型. 范畴论，尤其是 topos 理论把辩证法引入数学以及与数学有关的科学，使人们能用具体化数学化的辩证法去指导自己学习运用发展数学的实践. 这正是 Lawvere 意义下的数学基础 (foundation of mathematics).

Lawvere 对什么是数学基础有一个很明晰但与众不同的认识. 他认为传统的数学基础的研究只是数学的一个分支, 即 subjective logic, 而不是数学基础. 他认为数学基础应该帮助人们对数学有一个整体的了解, 教给大家一定的看问题分析问题的方法, 以指导人们去学习应用发展数学. 而范畴论, topos 理论正是具有这样意义的 foundation 的一部分.

1989 年夏天在英国剑桥大学举行的一个讨论范畴论的哲学意义的会议上 Lawvere 说: Why must we study the foundation of mathematics? Why must we study the history of mathematics? According to my interpretation we must study the history of mathematics in order to arrive at the foundation of mathematics, in order to discover the laws of the development of scientific thought, objective as well as subjective. Why must we know these laws? Above all to arrive at a position from which we can teach these laws. And why teach them? In order to assist the learning, development and utilization of mathematics itself, that is the science of space and quantity.

这章分为三节, 1. Topos 理论和范畴论的唯物论的意义; 2. 变化与联系; 3. 辩证法的形式化.

## §1 Topos 理论和范畴论的唯物论的意义

17 世纪牛顿、莱布尼兹创立的微积分在当时并不严格, 没有极限的定义. 但是运算简便, 利用微积分求导为物理量的计算提供了很大方便. 后来微积分的进一步发展要求严格化. 集合论的引进是数学发展的一个进步, 是数学严格化的要求. 随着数学的不断发展, 以集合论为基础的数学却暴露出它的许多局限性. 根据集合论将一个空间 (物理实体) 分为孤立点的集合, 然后放入某种数学

结构将这些点粘起来；把物体的连续运动分解为不连续的运动，再用极限过程将其连续起来. 这使很多运算变得很复杂. 这在研究较为简单的牛顿力学刚体运动时起了很好的作用，但在进一步研究连续力学时，状态空间是复杂的微分流形，讨论微分流形上的微分积分，讨论流形间的相互关系时，再完全还原到孤立点间断运动的作法就非常不实际，甚至行不通. 对进一步发展起来的连续变化的数学结构如复盖空间 (covering space), 层 (sheaf), 向量丛 (vector bundle), 切向量丛 (tangent bundle) 等用这种集合论还原法是非常困难的. 怎样使变化的数学结构的研究既有严格的数学理论，又有牛顿、莱布尼兹当时的简明直接的方法，使之能为物理学及其他科学提供更深刻更精确地反映客观世界的，有决定性、抽象性、一般性关系的数学模型，就成为问题.

Topos 理论的引入正是基于这一考虑. 把具有内结构的空间，把连续变化的物理对象直接作为研究对象，作为几何实体，用几条简单的公理对空间的范畴和量的范畴加以规定，而不用还原到集合论. 这样，连续映射或其它具有很好性质的映射如可微分，光滑映射等就成为范畴内的映射，而不用另加复杂的规定.

"The theory of topos is a basis for the study of continuously variable structures, as classical set theory is a basis for the study of constant structures"(Lawvere, Continuously variable sets; Algebraic geometry=Geometric logic, Proceedings of the Logic Colloquium, Bristol, 1973, North-Holland)

整个科学发展的图象是外部运动着的物质世界与人脑这一思考着的物质的相互作用. 人脑思考的功能就是要找出世界发展及某一具体过程研究对象的有决定意义的、抽象的、一般的关系 (decisive, abstract, general relation), 对此进行学习研究. 而抽象的一般的关系往往表现为数学关系，以数学手段对这些关系加以研究得出结论用以指导人类的生产实践活动与对自然界的进一步认识.

数学是人类对空间形式和数量关系以及它们的联系与转化的研究的科学. 范畴论为从整体上研究空间形式与数量关系的联系与转化提供了一个有力的工具. 范畴论强调要真正认识某一数学结构不能只是静止地孤立地研究这一数学结构, 更重要的是通过了解这一结构与其他结构的联系及转化加以研究. 为了更精确地用数学反映这些决定性、抽象性、一般性的关系, 尤其在物理学上的关系, 就需要一个卡氏积封闭的 (cartesian closed) 范畴, 即要求函数空间的存在; 为了直接地而不是回到集合论去做分析、逻辑推理就需要有真值对象 (truth value object); 为了能作出各种数学结构与范畴内及范畴之间的很多数学构造就需要有有限极限与上极限. 有有限极限, 卡氏积封闭, 有真值对象, 这正是 topos 定义中的三条公理. 下面分别对这三条公理加以说明.

在最开始的的 topos 定义中, 有限上极限的存在是作为一条公理给出的. 后来证明由 topos 的其它三条公理可以推出有限上极限的存在.

极限或上极限是一种具有 universal mapping 性质的结构. 在一个范畴 $C$ 内, 若任一对具有相同定义域与 codomain 的映射都具有 equalizer, 并且有限乘积存在, 那么可推出在这一范畴 $C$ 内任意有限极限存在. 特别 terminal 对象存在, 两个对象的卡氏积存在, 于是可以在 $C$ 内直接定义如半群, 群, 环, 模等代数结构. 范畴内与范畴之间的不少概念构造, 如 fiberization, 正交 (orthogonal), comma 范畴, Kan extension, 以及范畴的各种内结构, 内逻辑的一些相应的概念与构造, 都需要不同类型的极限, 上极限.

卡氏积闭合即要求函数空间在范畴内存在. $X,Y$ 是两个空间, $X$ 到 $Y$ 的全体 (连续) 映射 $Y^X$ 也是一个空间. $Y^X$ 称为函数空间, 并且 $Z\times X$ 到 $Y$ 的映射一一自然对应于 $Z$ 到 $Y^X$ 的映射

$$\frac{Z \times X \longrightarrow Y}{Z \longrightarrow Y^X}$$

这正是泛函分析的基本要求. 又如在物理中 $E$ 是一般物理空间, 如三维欧氏空间, $B$ 代表一个特殊的物体, $T$ 是一维时间. 这样 $B\times T$ 到 $E$ 的一个函数 $f: B\times T \longrightarrow E$ 刻画了物体 $B$ 在空间 $E$ 中的运动, $f(x,t)$ 告诉我们在时刻 $t$ 物体 $B$ 上 $x$ 点在空间 $E$ 中的位置. 有时我们需要将 $B$ 的这一运动 $f$ 描述为 $\overline{f}: B \longrightarrow E^T$, 这里 $E^T$ 是一个函数空间, 它代表 $E$ 上所有可能的点的运动轨迹, $E^T$ 独立于 $B$ 而存在. 通过函数 $\overline{f}$ 可以强调 $B$ 上每一点的运动轨迹. 有时又需要将 $f$ 描述为 $\overline{\overline{f}}: T \longrightarrow E^B$, 这里 $E^B$ 也是函数空间, 是物体 $B$ 在空间 $E$ 中所有可能占据的位置, 它独立于时间 $T$. $\overline{\overline{f}}(t)$ 给出在时刻 $t$, $B$ 在 $E$ 中的位置. 函数 $f$ 和它的不同表现形式 $\overline{f}, \overline{\overline{f}}$ 都是物理学中, 泛函分析中所必需的且习以为常的.

一个对象 $X$ 的子对象构成一个 preordered 集合. Topos 有真值对象 $\Omega$, 这使得 $X$ 的子对象成为可代表的 (representable), 这就是说, $X$ 的一个子对象 $A \hookrightarrow X$ 对应于一个从 $X$ 到 $\Omega$ 的映射 $\varphi_A: X \longrightarrow \Omega$,

$$\begin{array}{ccc} A & \hookrightarrow & X \\ \downarrow & & \downarrow \varphi_A \\ 1 & \xrightarrow{t} & \Omega \end{array}$$

这是一个 pullback 图形. 又由于 topos 是卡氏积闭合的, 所以函数空间 $\Omega^X$ 是 $X$ 的子对象的对象 (不是集合). $\Omega$ 本身是一个内 Heyting 代数对象, $\Omega$ 的交 $\wedge: \Omega\times\Omega \longrightarrow \Omega$, 并 $\vee: \Omega\times\Omega \longrightarrow \Omega$, 否定 $\neg: \Omega \longrightarrow \Omega$, Heyting 运算 $\Longrightarrow: \Omega\times\Omega \longrightarrow \Omega$, 这些运算与特征函数 $\varphi_A, \varphi_B$ 的合成, 给出 $X$ 的子对象 $A\wedge B$, $A\vee B$, $\neg A$, $A \Longrightarrow B$. $x \longrightarrow 1$ 与 $t: 1 \longrightarrow \Omega$(真),$f: 1 \longrightarrow \Omega$ (假) 的合成给出

$\Omega^X$ 中的真 $t_X$(全集), 假 $f_X$(空集). 这样 $\Omega^X$ 成为一个内 Hegting 代数对象, 这就是说对这个 topos $\mathcal{E}$ 中的任一对象 $Y$, $Y$ 到 $\Omega^X$ 的所有映射 $\mathcal{E}(Y, \Omega^X)$ 是一个 Heyting 代数. 由于一般 topos 中的真值对象 $\Omega$ 不是二值的, 即一般 topos 中的内逻辑不是经典的 (布尔值的), 所以选择公理, 排中律一般不成立. 一般 topos 的内逻辑是所谓的直觉 (intnitionistic) 多值逻辑. 由集合及其映射作成的范畴 $\mathcal{S}$ 也是一个 topos, 它的真值对象 $\Omega = \mathbf{2} = \{$ 真, 假 $\}$, 只有两个值, 而经典布尔值的逻辑正是范畴 $\mathcal{S}$ 的内逻辑.

范畴论的基本概念映射是 (广义) 元素 (请参考第 12 章, 及本章第 2 节), 映射的合成给出元素的归属关系; 数学构造的存在是具有某种性质的映射或函子的存在; 公理定理等等是某种范畴性质的构造的存在以及映射构成的图形的可换, 就成为具有一定性质的元素的存在以及元素的相等关系. 这样一般数学家所习以为常的逻辑语言, 即用元素隶属关系的叙述证明方法, 只要注意到没有用到选择公理与排中律, 就可以完全搬到任一 topos 中来. 用连续变化的集合的范畴 (topos) 作为连续力学, 热动力学以及其他学科的数学模型, 就与用常量集合作的数学模型具有同样直观简便的方法.

## §2 变化与联系

经典集合论的基本概念是元素以及元素的归属关系. 对数学结构的经典研究一般是对数学结构的孤立的研究. 后来由于不同数学分支方法结构的相互渗透, 如代数拓扑、代数几何等, 就需要了解相同结构和不同结构之间的联系与转化, 于是有范畴, 函子, 自然变换等概念的提出. 一种数学结构与保持此种结构的映射构成一个范畴. 如代数结构: 群, 环, 域, 模, 向量空间, 代数等, 几何结构: 拓扑, 度量空间, 可测空间等、与保持此种结构的映射

构成所谓具体 (concrete) 范畴. 不同数学结构之间的转化成为范畴之间的函子, 如基本群 (fundamental group), 同调上同调函子, 各种理论的模型等. 不同转化之间的联系是函子间的自然变换.

$S$ 是集合和集合之间映射构成的范畴. $X$ 是一个集合, $X$ 的一个元素 $x \in X$ 是由一个元素的集合 1 到 $X$ 的一个映射 $x: 1 \longrightarrow X$. 对于一个数学结构如群、环, 拓扑空间等, 只知道它的元素是远远不够的. 要描述它的内部结构, 元素的内聚性 (coherence), 需要了解其他对象到它以及它到其他对象的映射. 例如 $X$ 是一个拓扑空间. 让 $S$ 为 Sierpinski 空间, $S$ 有两个元素 $\{0,1\}$, 其中 $\{0\}$ 是开集, $\{1\}$ 是闭集. 这样 $X$ 到 $S$ 的一个连续映射对应于 $X$ 的一个开集, $X$ 到 $S$ 的连续映射的集合 $\mathrm{Top}(X,S)$ 给出 $X$ 的所有开集的集合. 一个可三角化 (trianglization) 的拓扑空间, 它的拓扑结构可以由 $\{n\text{-cell} \mid n=0,1,2,\cdots\}$ 到它的连续映射所决定.

把映射作为基本概念, Lawvere 在 1964 年给出与经典集合论公理等价的集合论范畴的公理 (见 [1]).

在任一范畴 $C$ 内, 我们定义由 $C$ 中任意对象 $Y$ 到 $X$ 的一个映射 $x: Y \longrightarrow X$ 是 $X$ 的一个广义元素 (generalized element), 记为 $x \in X$. 很多时候我们就称其为元素. 这样我们可以说 $X$ 由它的元素所决定.

70 年代初, Lawvere 和 Tierney 提出 topos 的概念. 一个 topos 从某种意义上说是一个推广了的集合论. 由以上定义的元素概念可以运用人们已熟悉了的经典集合论的元素归属的语言去描述数学概念和结构, 又由 topos 的逻辑特性, 可做相应的逻辑推理.

联系变化转化的一个重要概念是 adjoint functors. 在代数中 $\mathcal{G}\mathrm{ps}$ 是群与群同态的范畴, $\mathcal{S}$ 是集合的范畴. $U: \mathcal{G}\mathrm{ps} \longrightarrow \mathcal{S}$ 为 forgetful 函子, $U$ 的 left adjoint $F: \mathcal{S} \longrightarrow \mathcal{G}\mathrm{ps}$ 即是自由群函子. $B$ 是一个集合, $F(B)$ 就是 $B$ 生成的自由群. 这对于其它一些数学结构的“自由”构造也是对的, 自由构造定义为到 $\mathcal{S}$ 的 forgetful

函子的 left adjoint.

让 Ab 为可换群的范畴. $i$ : Ab $\longrightarrow$ $G$ps 是嵌入. $i$ 的 left adjoint 是所谓 commutator

$$G \longrightarrow G/[G,G].$$

在几何中, Top 为拓扑空间和连续映射的范畴. $X$ 是一个拓扑空间, $B$ 是一个集合.

discrete: $\mathcal{S} \longrightarrow$ Top, discrete($B$) 具有离散拓扑,

codiscrete: $\mathcal{S} \longrightarrow$ Top, codiscrete($B$) 具有非离散拓扑,

pt: Top$\longrightarrow \mathcal{S}$, pt($X$) 是拓扑空间 $X$ 的点的集合.

这里, codiscrete 是 pt 的 left adjoint, 而 pt 是 discrete 的 left adjoint.

在代数几何中, $K$ 是一个代数闭域. $\mathrm{Alg}_K$ 是 $K$ 上代数的范畴, Scheme 是 $K$ 上 scheme 的范畴, 可换环的 spectrum 构造给出从 $K$- 代数到 Scheme 的一个函子, 而 global section 函子 $\Gamma$ 给出从 Scheme 到 $K$- 代数的一个函子.

$$\mathrm{Alg}_K^{\mathrm{op}} \underset{\Gamma}{\overset{\mathrm{Spec}}{\rightleftarrows}} \mathrm{Scheme}$$

spec 是 $\Gamma$ 的 left adjoint, 这给出了代数与几何之间的一个联系.

我们看到很多数学结构如 commutator, 离散拓扑, 非离散拓扑, spectrum 等等本身就是函子, 即是一个映射. 又如 $G$ 是一个群, $G$ 作用在一个集合 $B$ 上, $B$ 成为一个 $G$–set. 若 $G$ 是不可换的, 左 $G$–set 是函子 $B$ : $G \longrightarrow \mathcal{S}$, 右 $G$–set 为函子 $B$ : $G^{\mathrm{op}} \longrightarrow \mathcal{S}$. $G$–set 之间保持 $G$ 作用的映射即为相应函子之间的自然变换. 模型是从一个小范畴 (理论) 到 $\mathcal{S}$ 或其它范畴的具有一定性质的函子. 例如代数理论的模型一般是要求这个函子保持乘积. 而模型之间的映射成为相应函子之间的自然变换.

## §3 辩证法的形式化

这里不去一般地讨论这一问题，而是讨论辩证法的一些基本范畴在 topos 理论中的具体体现，以及对这些基本范畴的理解带来的对数学学习研究的指导意义. 这些基本范畴包括：特殊和一般，空间和数量，外延量与内涵量 (extensive quantity and intensive quantity).

(1) 一个 topos 同时具有几何和逻辑的特性. 从几何意义上说 topos 有两种，一种是作为一个特殊空间的 topos, 例如一个拓扑空间 $X$ 上的 sheaf 构成的范畴 $\mathrm{Sh}(X)$, 或空间 $X$ 上的丛 (bundle) $\mathcal{E}/X$; 二是作为一般空间的范畴，如 Johnston topos(拓扑空间), Grothendieck 的解析空间的范畴，组合 (combinatorial) 空间的范畴等. 作为特殊空间的 topos 与作为一般空间的 topos 有很不相同的性质，这可以用一组公理来区别.

我们知道从拓扑空间与连续映射的范畴 Top 到集合的范畴 $S$ 有一个 forgetful 函子 (又称为点函子 pt) $\Gamma_* :\ \mathrm{Top} \longrightarrow S$. 如果 $B$ 是一个集合，有两种不同的方法去构造 $B$ 上的平凡拓扑 (trivial topology). 一种是离散拓扑即 $B$ 中每一点都是一个开集；另一种是非离散拓扑即 $B$ 中所有的点都被粘在一起，开集只有全集和空集. 具有非离散拓扑的空间又称为 chaotic 空间，因为所有的点都被粘在一块，关于空间本身结构的任何信息都得不到，所以空间是混乱的. 这里记离散空间函子 discrete 为 $\Gamma^*$, 非离散空间函子 codiscrete 为 $\Gamma^!$. 这样 $\Gamma^*$ 是 $\Gamma_*$ 的 left adjoint, $\Gamma_*$ 是 $\Gamma^!$ 的 left adjoint.

$$\frac{\Gamma^*(B) \longrightarrow X}{B \longrightarrow \Gamma_*(X)} \qquad\qquad \frac{\Gamma_*(X) \longrightarrow B}{X \longrightarrow \Gamma^!(B)}$$

一般 $\mathcal{S}$ 上的 topos $\mathcal{E}$ 都具有 $\mathcal{E}$ 到 $\mathcal{S}$ 的一个 forgetful 函子 $\Gamma_*: \mathcal{E} \longrightarrow \mathcal{S}$, 以及 "离散空间" 函子 $\Gamma^*: \mathcal{S} \longrightarrow \mathcal{E}$, 但是不一定有 "非离散空间" 函子 $\Gamma^!$, 这就是说 $\Gamma_*$ 有 left adjoint $\Gamma^*$, 但一不定有 right adjoint $\Gamma^!$. 例如 topos Sh($X$) 就不具有 $\Gamma^!$. 这样作为一般空间的 topos 第一条公理就是 "非离散空间" 函子 $\Gamma^!$ 存在.

第二条公理是为从量的空间到质的空间的转化即同伦 (homotopy) 的构造所必需的. 拓扑空间的同伦群 (基本群) 给出了拓扑空间的一个不变量. 用同伦的概念可以区分具有不同连通性这样本质不同的空间. 两个拓扑空间 $X,Y$ 是同伦等价的若它们有同构的同伦群, 同时用同伦概念可以划分连续映射为同伦类. 这样就有从量到质的转变, 从拓扑空间的范畴 Top 过渡到同伦等价空间的范畴 [Top]. 在 [Top] 中同伦等价的空间被看为同一个空间, 而映射则是连续映射的同伦类. 这样同伦的概念是一般空间的 topos 所应具有的概念. 同伦的概念在一般空间的 topos $\mathcal{E}$ 中就成为要求连通分支函子 (connected component) $\pi_0$ 存在, 并且 $\pi_0$ 保持有限乘积. 连通分支函子 $\pi_0$ 是离散空间函子 $\Gamma^*$ 的 left adjoint. $\mathcal{E}$ 中两个空间 $X,Y$ 若具有同样的连通分支空间 $\pi_0(X) \approx \pi_0(Y)$, 即 $X,Y$ 在同伦范畴 $[\mathcal{E}]$ 中同构. $X$ 到 $Y$ 的函数空间 $Y^X$ 的同伦空间 $\pi_0(Y^X)$ 正是 $X$ 到 $Y$ 的连续映射的同伦类空间. 由于 $\pi_0$ 保持乘积, 这样就有

$$\pi_0(Y^X \times Z^Y) \approx \pi_0(Y^X) \times \pi_0(Z^Y),$$

这给出了同伦类的复合

$$\pi_0(Y^X) \times \pi_0(Z^Y) \approx \pi_0(Y^X \times Z^Y) \longrightarrow \pi_0(Z^X)$$

一般空间的 topos $\mathcal{E}$ 过渡到它的同伦类的范畴 $[\mathcal{E}]$, $[\mathcal{E}]$ 和 $\mathcal{E}$ 具有同样的对象, 但 $[\mathcal{E}](X,Y) = \pi_0(Y^X)$.

第三条公理是要求真值对象是简单连通的, 即 $\pi_0(\Omega) = 1$. 这样对于任一空间 $X$, $\pi_0(\Omega^X) = 1$. 因为从任一空间 $X$ 有一自然嵌

入 $X \longrightarrow \Omega^X$, $X$ 可以嵌入一个简单连通空间 $\Omega^X$. 这样就把布尔值的 topos 排除在外, 因为对布尔值的 topos, 例如集合的范畴 $\mathcal{S}$, $\Omega = \mathbf{2} = 1 + 1$, 而 $\pi_0(1+1) = \pi_0(1) + \pi_0(1)$.

一般空间的 topos 的一个简单例子. 让 $\Delta = \{1, \partial_0, \partial_1\}$ 是三个元素的有单位元的半群 (monoid), $\partial_i \partial_j = \partial_i$, $i = 0, 1$. 这样函子范畴 $\mathcal{S}^{\Delta^{op}}$ 是满足一般空间 topos 的三条公理的. $\mathcal{S}^{\Delta^{op}}$ 中的对象称为 reflexive graph.

一般空间的 topos $\mathcal{E}$ 和一个特殊空间的 topos, 如 $\mathcal{E}$ 中某一空间 $X$ 上 sheaf 构成 topos Sh($X$) 之间的关系, 即一般与特殊空间之间的转化关系是一对 adjoint 函子

$$\mathcal{E} \underset{f_*}{\overset{f^*}{\rightleftarrows}} \mathrm{Sh}(X)$$

这里 $f_*$ 是一个嵌入, 而 $f^*$ 是所谓 sheaf 化函子, $f^*$ 是 $f_*$ 的 left adjoint.

这样在为物理学, 计算机科学等学科中的问题选择数学模型时, 就能根据问题性质选择一般或特殊空间的 topos.

(2) 空间和 (数) 量 (space and quantity)

我们生活于物质世界上并能在其中运动, 这称为空间; 而运动的结果称为 (数) 量.

空间是几何性质的, 这里包括作为一般空间的范畴与作为特殊空间的范畴. 几何图形是满足分配律的: $A \times (B + C) \approx (A \times B) + (A \times C)$. 这里

$A \times B$ 是 $A$ 与 $B$ 的乘积 (product),

$A + B$ 是 $A$ 与 $B$ 的和 (coproduct).

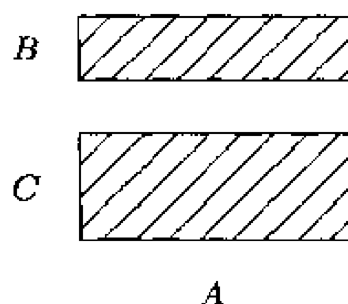
当然在不同的范畴中乘积与和的构造不同. 例如在拓扑空间的范畴 Top 中, 乘积即是卡氏积, 而两个空间的和是不交并. 例如

$A$ 是直线 ______________,

$B$ 是直线 ____,

$C$ 是直线 ______,

那么下图给出 $A \times (B + C)$




但这正是 $(A \times B) + (A \times C)$, 即有

$$A \times (B + C) \approx (A \times B) + (A \times C).$$

一般空间的范畴都是满足分配律的. 如离散空间即集合的范畴, 拓扑空间的范畴, 可微分流形的范畴, 可度量空间的范畴, 组合空间的范畴等. 一个推广了的空间如拓扑空间 $X$ 上的 sheaf 的范畴 $\mathrm{Sh}(X)$, $X$ 上复盖空间的范畴都反映了空间 $X$ 的性质, 而这些广义空间的范畴也是满足分配律的.

一个满足分配律以及以下几个性质的范畴 $\mathbf{D}$ 称为一个分配范畴 (distributive category),

1) $\mathbf{D}/X$ 也是满足分配律的, 这里 $X$ 是 $\mathbf{D}$ 中任一对象,

2) $\mathbf{D}/0 \approx 1$,

3) $\mathbf{D}/X \times \mathbf{D}/Y \approx \mathbf{D}/(X + Y)$.

每一个 topos 都是一个分配范畴. 分配范畴是空间的范畴.

一个空间上的量总是可加的, 并且具有一个数乘运算. 例如一个空间上实数性质的量 $\tau$ 与一个实数 $k$ 的乘积 $k\tau$ 仍是这个空间上的一个量, 这样量的范畴具有线性性质, 如一个域 $F$ 上的线性空间和线性变换的范畴 $\mathbf{V}_F$. 这样的范畴与分配范畴很不相同,

首先它不满足分配律. 例如 $\mathbf{V}_F$, $F$ 是 $F$ 上的一维线性空间, 让 $A=B=C=F$, 那么 $A\times(B+C)=F\times(F+F)=F^3$, 而 $(A\times B)+(A\times C)=(F\times F)+(F\times F)=F^4$, 这是因为在 $\mathbf{V}_F$ 中乘积与和的构造是一样的.

一个可换环 $R$ 上的模的范畴 $R$-mod 也具有与 $\mathbf{V}_F$ 同样的线性性质. 拓扑空间 $X$ 上实值或复值连续函数可以看为是 $\mathbf{R}$ 或 $\mathbf{C}$ 上的模, 这正是 $X$ 上的量.

这样量 (数量) 的范畴应该是线性的. 线性范畴的公理是从线性空间和线性变换的范畴的性质中提炼出来的. 线性范畴的公理有两条:

1) $1\approx 0$,

2) $A\times B\approx A+B$.

除线性空间和环上模外, 拓扑向量空间, bornlogical 空间, 射影模的范畴, 向量丛的范畴都是线性的.

线性范畴的第一条公理是说 terminal object 1 与 initial object 0 同构. 我们称这个对象为零元素. 记为 0. 零元素具有性质, $A$ 是这个线性范畴中的任一对象, 有 $A$ 到 0 的唯一映射并且有 0 到 $A$ 的唯一映射

$$A\longrightarrow 0,\qquad 0\longrightarrow A.$$

若 $B$ 是另一个对象, 那么存在 $A$ 到 $B$ 的一个映射 $0_{AB}: A\longrightarrow 0\longrightarrow B$. 由和的性质, 我们知道有 codiagonal 映射 $\nabla: A+A\longrightarrow A$, 但是 $A+A\approx A\times A$, 所以 $A$ 上有加法

$$\underbrace{A\times A\approx A+A\xrightarrow{\nabla}A}_{+},$$

而 $0_A: 1\approx 0\longrightarrow A$ 是单位元. 这样 $A$ 成为一个 monoid.

如果 $f,g$ 是 $B$ 到 $A$ 的两个映射, $f,g: B\longrightarrow A$, 可以定义 $f+g=+\circ(f\times g): B\times B\xrightarrow{f\times g}A\times A\xrightarrow{+}A$, 而 $0_{BA}: B\longrightarrow 0\longrightarrow A$

是单位元. 我们记这个线性范畴为 $\mathbf{L}$, 那么 $\mathbf{L}(B,A)$ 是一个 monoid. 可以认为 $\mathbf{L}(B,A)$ 是一个量的系统或数量系统, 就像 $\mathbf{L}(1,\mathbf{R})$ 是数量系统一样, 这里 $\mathbf{R}$ 是实数域. 在几何中这些量可以是维数或不同的张量丛等, 在物理上这些量可以是质量, 长度, 时间, 密度, 压力, 能量等等.

这样空间的范畴是分配范畴, 而量的范畴是线性范畴. 空间的范畴 $\mathbf{D}$ 与量的范畴 $\mathbf{L}$ 的基本关系是, 量的系统 $\mathbf{L}(B,A)$ 也是一个空间, 即 $\mathbf{L}(B,A)$ 是 $\mathbf{D}$ 中一个对象 (这正是函数空间的意义). 而量的系统的复合 $\mathbf{L}(A,B)\times\mathbf{L}(B,C)\longrightarrow\mathbf{L}(A,C)$ 也是 $\mathbf{D}$ 中的一个映射. 这一关系又称为线性范畴 $\mathbf{L}$ 是 enriched in 空间的范畴 $\mathbf{D}$.

量 (数量) 在空间上变化. 这里空间可以是一般空间范畴的一个对象, 也可以是一个特殊空间的 topos 如 $\mathrm{Sh}(X)$. 空间起的作用有两个, 一是作为运动状态或运动地点的空间, 另一是作为变化着的量 (数量) 的定义域. 第二点将在下面内含量和外延量中作进一步说明.

(3) 内含量 (intensive quantity) 和外延量 (extensive quantity)

一个空间 $X$ 上的外延量是这个空间的整体性质. 如物理上的体积, 质量, 能量; 数学上的各种测度等. 而内含量是一种局部的性质, 是定义于空间上每一点的函数如密度, 温度, 以及空间 $X$ 上的各种实值、复值连续、可测函数等. 内含量一般是外延量的比值. 例如密度是质量对体积的比值. 又如 Radon-Nikodym 定理: 两个满足一定性质的测度的比值是一可测函数.

外延量是协变的: $f$ 是从空间 $X$ 到空间 $Y$ 的一个连续映射, 那么 $f$ 会导致一个从 $X$ 上的外延量 $E(X)$ 到 $Y$ 的外延量 $E(Y)$ 的映射

$$E(f):\ E(X)\longrightarrow E(Y).$$

而内含量是反变的: 同样的 $f$ 会导致一个 $Y$ 上的内含量 $C(Y)$ 到

$X$ 上内含量 $C(X)$ 的一个映射

$$C(f):\ C(Y) \longrightarrow C(X).$$

更一般地说, 一个外延量的类型 (type of extensive quantity) 是从空间的范畴 $\mathbf{D}$ 到量的范畴 $\mathbf{L}$ 的一个保持和 (coproduct) 的协变函子 $E$. 保持和是说若空间 $X$ 分为两个不相交空间 $X = X_1 + X_2$, 那么 $E(X) \approx E(X_1) + E(X_2)$, $X$ 上的一个测度完全由这一测度在两个部分空间 $X_1, X_2$ 上的度量所决定.

对于只含一个点的空间 1, $E(1)$ 给出这个外延量类型的总值. 因为从任一空间 $X$ 存在到一个元素的空间 1 的唯一映射 $X \longrightarrow 1$, 这样就有映射 $E(X) \longrightarrow E(1)$, 它给出空间 $X$ 上的任一属于这一类型外延量 $\tau \in E(X)$ 的总值.

空间 $X$ 上的任意一点 $x:\ 1 \longrightarrow X$ 给出 $X$ 上的一个 Dirac 测度 $\delta_x$,

$$\delta_x(B) = \begin{cases} 1, & 若\ x \in B, \\ 0, & 若\ x \notin B. \end{cases}$$

一个内含量的类型是从空间的范畴 $\mathbf{D}$ 到量的范畴 $\mathbf{L}$ 的一个反变函子 $C$. 对于一个元素的空间 1, $C(1)$ 是常量, 或者说 $C(1)$ 是这一类型内含量的值域, $C(1)$ 常常是一个环. 空间 $X$ 到一个元素空间 1 的唯一映射 $X \longrightarrow 1$ 导致常量 $C(1)$ 到 $X$ 上的内含量 $C(X)$ 的嵌入 $C(1) \longrightarrow C(X)$, 这就是说任一常量 (常函数) 也是一个内含量.

空间 $X$ 上的任意一点 $x:\ 1 \longrightarrow X$, 有 $C(X)$ 到常量 $C(1)$ 的一个映射称为 evaluation $\mathrm{ev}_x:\ C(X) \longrightarrow C(1)$, $\mathrm{ev}_x$ 将 $X$ 上的任一内含量 $g \in C(X)$ 送到它在 $x$ 点的值 $\mathrm{ev}_x(g) = g(x)$. 一般来说 $X$ 上的内含量的类型 $C(X)$ 是一个环.

内含量与外延量的基本关系是, 内含量作用于外延量而产生新的外延量. 例如在泛函分析中 $\mu$ 是空间 $X$ 上的一个测度即一个

外延量，$g$ 是 $X$ 上的一个连续实值或复值函数，$g$ 是内含量. 这样对 $X$ 的任一可测子空间 $A$, 定义

$$\mu_g(A) = \int_A g\, d\mu.$$

$\mu_g$ 是空间 $X$ 上的一个新的外延量. 例如 $g$ 是密度函数，$\mu$ 为体积测度，那么 $\mu_g$ 是质量分布.

内含量与外延量的这一关系在代数拓扑中称为 projective formula, 在群表示论中称为 Frobenius reciprocity, 在量子力学中称为 covariance 或 canonical commutation relation. 内含量与外延量的这一关系又可以表示为外延量 $E(X)$ 是内含量 $C(X)$ 上的一个模.

$$\begin{aligned} C(X) \times E(X) &\longrightarrow E(X) \\ (g, \mu) &\longmapsto \mu_g. \end{aligned}$$

这种模结构要求对外延量或内含量有一定的限制. 例如，$X$ 是拓扑空间. 我们取内含量为 $X$ 上的实值连续函数 $C(X) = \mathrm{Top}(X, \mathbf{R})$. 这在拓扑空间和连续映射的范畴 Top 中没有任何限制. 而对 $X$ 上的外延量 $E(X)$ 限制为 Radon 测度且具有紧致支撑 (compact support). 这样如上的这种模结构就很自然. 但如果像不少书上那样 (例如 Bourbaki) 限制内含量 $C(X)$ 为具有有限支撑的连续函数，而对外延量不加限制，那么这种模结构的存在就成为一个问题.

当由量的空间过渡到质的空间时，即由空间的范畴 **D** 过渡到同伦的范畴 [**D**] 时，空间 $X$ 上的内含量与外延量相应地过渡到 $X$ 上的上同调 (cohomology) 与同调 (homology). 上同调是内含量是反变的，同调是外延量是协变的，并且上同调作用于同调.

其它辩证法的范畴如 Being 与 Becoming, 量变与质变，抽象与具体等也在范畴论，topos 理论中有具体体现. 这里就不具体讨论了. 请见 [2],[4] 及其中所引诸文献.

世界的发展是辩证的. 近代科学的发展, 边缘学科的兴起使辩证思维成为必需. 运用范畴, 函子, 自然变换, adjoint functors, closed category, enriched category, topos 等等概念, 可以具体化形式化辩证法的有关范畴, 使人们可以用它来指导自己学习, 应用, 发展数学的实践.

不应该只是将范畴论作为数学的一个分科来学习和研究. 范畴论还是一种方法论, 它为我们提供了一种从全局, 整体地看问题分析问题的方法; 范畴论是研究联系, 变化, 转化的工具. 人们正在认识到范畴论是现代数学和与数学有密切联系的学科的语言和语法.

## 参考文献


1 Lawvere F W. An elementary theory of the category of sets. Proc. National Acad. Sci. U.S.A., 1964, 52: 1506~1511

2 Lawvere F W. Tools for the advancement of objective logic: closed categories and toposes. The Logical Foundations of Cognition (Edited by Macnamara J and Reyes G E). Oxford: Oxford Univ. Press, 1994, 43~56

3 McLarty C. The uses and abuses of the history of topos theory. British Jour. for the Philosophy of Science, 1990, 41: 351~375

4 孟晓青. Topos 理论的哲学意义及辩证法的形式化. 哲学动态, (1994 增刊), 77~82

5 Lawvere F W. Adjointness in foundations. Dialectica, 1969, 23: 281~296